Universiteit Gent
Faculteit Wetenschappen
Vakgroep Wiskunde: Analyse, Logica en Discrete Wiskunde

Karakterisering van codewoorden van incidentiecodes komende van projectieve ruimten

Pauline Vanden Eede

UNIVERSITEIT
GENT

Academiejaar 2023–2024

Promotor: prof. dr. Leo Storme

Masterproef ingediend tot het behalen
van de academische graad van master in de wiskunde

Voorwoord

Als iemand mij vijf jaar geleden had gezegd dat ik een masterproef zou schrijven over eindige meetkunde en codeertheorie had ik deze persoon waarschijnlijk raar aangekeken. Mijn beeld over wiskunde en de onderwerpen die ik kende, waren toen nog beperkt. Na gedurende mijn hele opleiding in contact te komen met verschillende takken van de wiskunde, ben ik echter heel blij om mijn masterproef over dit onderwerp te schrijven. Door de verbanden en terugkerende structuren is dit naar mijn mening één van de mooiste en interessantste domeinen in de wiskunde. Deze masterproef is voor mij dan ook voornamelijk een laatste ode aan mijn favoriete wiskundeonderdeel.

Voor we beginnen wil ik graag enkele personen bedanken. Als eerste wil ik mijn promotor prof. dr. Leo Storme bedanken om mij steeds te helpen en met veel geduld al mijn vragen te beantwoorden. Zijn enthousiasme en passie werkte aanstekelijk en zorgde ervoor dat ik telkens met plezier naar de besprekingen ging. Ook wil ik graag mijn ouders bedanken om mij te steunen tijdens het schrijven van deze masterproef. Dankjewel om steeds te vragen hoe het ging met mijn "boek" en voor de vele wandelingen. Daarnaast wil ik mijn vrienden bedanken voor de nodige ontspanning tussendoor. Ook een welgemeende bedankt aan mijn buurvrouw Josée voor het rotsvaste vertrouwen in mijn kunnen en de vele kaarsen tijdens de examenperiode. Ten slotte wil ik Jens Bossaert bedanken voor het ter beschikking stellen van dit LaTeX-template.

Pauline Vanden Eede
31 mei 2024

Inhoudsopgave

1 Inleiding

Deze masterproef gaat over de codes komende van incidentiematrices van structuren in projectieve ruimten. De hoofdrolspelers zijn de code $\mathcal{C}_k(n,q)$ en de bijhorende duale code $\mathcal{C}_k(n,q)^\perp$. In het volgende hoofdstuk zullen we deze codes formeel definiëren. We geven daar ook de definitie van enkele andere veel voorkomende begrippen. De codes $\mathcal{C}_k(n,q)$ en $\mathcal{C}_k(n,q)^\perp$ zijn doorheen de jaren veel bestudeerd. Desondanks zijn er ook nog veel zaken niet geweten. Zo is er veel onderzoek gedaan naar de gewichten die voorkomen in deze codes en welke codewoorden horen bij een bepaald gewicht. Hierbij werkt men van kleinere gewichten naar steeds grotere gewichten toe. Ook worden verbanden met k-blokkerende of even verzamelingen gebruikt. De wisselwerking met deze meetkundige structuren zorgt voor mooie resultaten. Samen met de ruimte voor nieuwe resultaten geeft dit aanleiding tot een interessant onderwerp. Wij zullen ons hier concentreren op deze karakterisering van codewoorden met een klein gewicht.

We beginnen met het kleinste niet-nul gewicht en de bijhorende codewoorden te bespreken. Het minimum gewicht van $\mathcal{C}_k(n,q)$ is gekend. We zullen bewijzen wat dit is in Hoofdstuk 3 en hoe de support van deze codewoorden eruit ziet. Echter niet voor alle waarden van q weten we wat het minimum gewicht is van $\mathcal{C}_k(n,q)^\perp$. De bespreking hierrond vormt het tweede deel van Hoofdstuk 3. Het zal blijken dat voor q priem of even het minimum gewicht gekend is. De vorm van de bijhorende codewoorden is gekarakteriseerd voor q priem en $q = 4$ of 8. We vergelijken daarnaast verschillende ondergrenzen voor het minimum gewicht van $\mathcal{C}_k(n,q)^\perp$ die doorheen de jaren bewezen zijn.

Recent zijn er verschillende doorbraken geweest in het classificeren van de codewoorden met een klein gewicht van $\mathcal{C}_k(n,q)$. In Hoofdstuk 4 bewijzen we één van de eerste resultaten hieromtrent. Dit toont aan dat er een leeg interval is in de verdeling van de gewichten. Daarnaast geven we in detail een kort bewijs voor de classificatie van de codewoorden tot gewicht $2q^{n-1}$ als $k = n-1$. In Hoofdstuk 5 bewijzen we nieuwe classificatie resultaten voor $\mathcal{C}_k(n,8)^\perp$, met $k \in \{1,\ldots,n-2\}$. Deze zijn gevonden in samenwerking met professor Leo Storme, de promotor van de auteur. We tonen aan dat codewoorden met een gewicht groter dan het minimum gewicht d, minstens gewicht $d+4$ hebben. Voor $q = 4$ vinden we partiële resultaten.

Ten slotte proeven we in het laatste hoofdstuk kort van enkele gerelateerde codes. Eerst overlopen we enkele resultaten over de codes $\mathcal{C}_{j,k}(n,q)$ en $\mathcal{C}_{j,k}(n,q)^\perp$. Vervolgens definiëren we op een andere manier onze incidentiematrix door incidentie te zien als snijden i.p.v. bevat zijn. We bespreken in detail een karakteriseringsresultaat voor de code van snijdende rechten in $\mathrm{PG}(3,q)$. Om te eindigen geven we een voorbeeld over codes van incidentiematrices komende van klassieke polaire ruimten. Dit hoofdstuk is slechts een tipje van de sluier om andere invalshoeken te illustreren. We hopen dat de lezer veel plezier beleefd aan deze masterproef over de wereld van codes gebaseerd op incidentiematrices en hierna zin heeft om verder in deze wereld te verblijven.

2 Basisbegrippen

In deze masterproef zullen we voornamelijk werken in de projectieve ruimte $\mathrm{PG}(n,q)$. Hierbij is $n \in \mathbb{N}$ de dimensie van de projectieve ruimte en q verwijst naar het veld $\mathbb{F}_q$ waarover we werken. Het getal q is in heel deze masterproef steeds een priemmacht, i.e. $q = p^h$, met p priem en $h \in \mathbb{N} \setminus \{0\}$. Een deelruimte met dimensie k, $k \in \{0, \ldots, n\}$, in deze projectieve ruimte noteren we korter als een k-ruimte. Het aantal punten van zo'n k-ruimte geven we weer met het gebruikelijke symbool θ_k. De Gaussische coëfficiënt $\begin{bmatrix} n+1 \\ k+1 \end{bmatrix}_q$ gebruiken we om het aantal k-ruimten in $\mathrm{PG}(n,q)$ weer te geven. Merk op dat $\theta_k = \begin{bmatrix} k+1 \\ 1 \end{bmatrix}_q$. We definiëren nu eerst de codes die we later zullen bestuderen. Nadien geven we de definities van enkele veelgebruikte meetkunde structuren. Dit hoofdstuk is gebaseerd op verschillende bronnen: [1], [2], [6],[14], [17], [22] en [26]. We gaan er vanuit dat de lezer achtergrondkennis heeft over codeertheorie en Galoismeetkunde zoals in de cursussen [38] en [39].

2.1. Codeertheorie

Kies gehele getallen j en k zodat $0 \leq j < k < n$. We kunnen dan de incidentiematrix G beschouwen waarvan de kolommen corresponderen met de j-ruimten σ en de rijen met de k-ruimten τ in $\mathrm{PG}(n,q)$. De waarde $G_{\tau,\sigma}$ is 1 als $\sigma \subset \tau$ en 0 als $\sigma \not\subset \tau$. De lineaire code voortgebracht door deze matrix over het veld $\mathbb{F}_p$ noteren we als $\mathcal{C}_{j,k}(n,q)$. Merk op dat de incidentiematrix geen generator is, want de rijen zijn niet noodzakelijk lineair onafhankelijk. Wanneer $j = 0$, gebruiken we de kortere schrijfwijze $\mathcal{C}_k(n,q)$. De duale code duiden we aan met $\mathcal{C}_{j,k}(n,q)^\perp$ en als $j = 0$ met $\mathcal{C}_k(n,q)^\perp$. Zoals vermeld in de inleiding, zullen wij voornamelijk werken met $j = 0$. Voor $j > 0$ vermelden we enkele gekende resultaten in deel 6.1. Laten we eerst enkele voorbeelden van codewoorden bespreken van $\mathcal{C}_k(n,q)$ om een betere intuïtie te vormen. Bij deze voorbeelden en ook later zijn we geïnteresseerd in de vorm van de support en het gewicht van het codewoord. De support van een codewoord c, $\mathrm{supp}(c)$, is de verzameling van de posities P zodat de coëfficiënt bij die positie, c_P, niet nul is. Het gewicht van dit codewoord, $w(c)$, is het aantal niet-nul posities. Zo is $w(c)$ gelijk aan de grootte van de verzameling $\mathrm{supp}(c)$. We beginnen met een eenvoudig voorbeeld.

Voorbeeld 2.1.1. Beschouw de code $\mathcal{C}_k(n,q)$ in $\mathrm{PG}(n,q)$. Per definitie wordt deze code voortgebracht door de incidentiematrix van punten P en k-ruimten τ. Elke rij G_τ correspondeert dus met de verzameling punten die in de k-ruimte τ liggen. We noteren dit als de karakteristieke vector χ_τ. We zullen deze vector soms ook de incidentievector noemen. Het is duidelijk dat dit een codewoord is van $\mathcal{C}_k(n,q)$. De bijhorende support is de k-ruimte τ in $\mathrm{PG}(n,q)$ en het gewicht is θ_k.

Ook voor de code $\mathcal{C}_{j,k}(n,q)$ associëren we met elke rij G_τ een karakteristieke vector χ_τ. We gebruiken later ook de karakteristieke vector van een verzameling. Deze is zoals men zou verwachten. Beschouw een verzameling $\mathcal{A}$ bestaande uit j-ruimten in $\mathrm{PG}(n,q)$. De karakteristieke vector $\chi_\mathcal{A}$ van de verzameling $\mathcal{A}$ is geïndexeerd over alle j-ruimten σ van $\mathrm{PG}(n,q)$. De j-ruimte σ heeft als coëfficiënt 1 wanneer $\sigma \in \mathcal{A}$ en anders 0. Af en toe zullen we deze vector ook korter noteren als

$\mathcal{A}$, net zoals we soms ook τ zullen gebruiken i.p.v. χ_τ. Het volgende voorbeeld bekomen we door het verschil van twee rijen uit de incidentiematrix G te nemen.

Voorbeeld 2.1.2. Het symmetrisch verschil van twee k-ruimten τ en τ' is de support van een codewoord c van $\mathcal{C}_k(n,q)$. Inderdaad, neem het verschil van de corresponderende rijen uit de incidentiematrix. De punten die in de doorsnede $\tau \cap \tau'$ liggen van de twee k-ruimten hebben coëfficiënt 0 in het nieuwe codewoord. De punten van τ en τ' buiten $\tau \cap \tau'$ hebben z.v.v.a. respectievelijk coefficiënt 1 en -1. Het gewicht van c wordt mede bepaald door $\dim(\tau \cap \tau')$. Afhankelijk van de grootte van k en n is het zelfs mogelijk dat $\tau \cap \tau' = \emptyset$ voor goedgekozen k-ruimten. In het algemeen is $w(\chi_\tau - \chi_{\tau'}) = w(\chi_\tau) + w(\chi_{\tau'}) - 2|\mathrm{supp}(\chi_\tau) \cap \mathrm{supp}(\chi'_\tau)| = 2\theta_k - 2\theta_{\dim(\tau\cap\tau')}$. Stel dat τ en τ' twee verschillende k-ruimten zijn die een $(k-1)$-ruimte gemeenschappelijk hebben. We vinden dan dat $w(c) = w(\chi_\tau - \chi_{\tau'}) = 2q^k$.

Merk op dat we vanaf nu ook minder rigoureuze verwoordingen zullen gebruiken zoals de k-ruimte τ is een codewoord i.p.v. de karakteristieke vector van de k-ruimte τ is een codewoord, om de tekst niet te overladen. We bespreken nu enkele voorbeelden van codewoorden van de code $\mathcal{C}_k(n,q)^\perp$. Een codewoord c behoort tot deze duale code als het orthogonaal is met elk codewoord $c' \in \mathcal{C}_k(n,q)$. We noteren het inproduct tussen twee codewoorden als (c,c'). Het is voldoende om enkel te controleren dat c orthogonaal is met de codewoorden die $C_k(n,q)$ voortbrengen. Dit wil zeggen dat het volstaat dat we nagaan of $(c,\chi_\tau) = 0$ voor alle k-ruimten τ. Het is dus duidelijk dat de nulvector $\mathbf{0}$ een codewoord is van $\mathcal{C}_k(n,q)^\perp$. We geven ook een minder eenvoudig voorbeeld.

Voorbeeld 2.1.3. In de code $\mathcal{C}_k(n,q)^\perp$ is het verschil van twee $(n-k)$-ruimten τ en τ' een codewoord. We controleren dat $(\chi_\tau - \chi_{\tau'}, \chi_\rho) = (\chi_\tau, \chi_\rho) - (\chi_{\tau'}, \chi_\rho) = 0$ voor alle k-ruimten ρ. Omdat we werken met karakteristieke vectoren zijn de coëfficiënten nul of één. Bijgevolg komt het berekenen van het inproduct overeen met het tellen van het aantal punten in de doorsnede van hun supports. In $\mathrm{PG}(n,q)$ snijden een k-ruimte en een $(n-k)$-ruimte minstens in een punt door de identiteit van Grassmann. Dus is $(\chi_\tau, \chi_\rho) = \theta_{\dim(\tau\cap\rho)} = 1 \pmod p$. Analoog is ook $(\chi_{\tau'}, \chi_\rho) = 1 \pmod p$ en bijgevolg $(\chi_\tau - \chi_{\tau'}, \chi_\rho) = (\chi_\tau, \chi_\rho) - (\chi_{\tau'}, \chi_\rho) = 1 - 1 = 0 \pmod p$. Opnieuw hangt af van $\dim(\tau \cap \tau')$ wat het gewicht is van het codewoord $\chi_\tau - \chi_{\tau'}$. We vinden dat $w(\chi_\tau - \chi_{\tau'}) = 2\theta_{n-k} - 2\theta_{\dim(\tau\cap\tau')}$.

Merk op dat de uitleg bij dit voorbeeld gebaseerd is op een speciaal geval van [26, lemma 1]. We kunnen bovenstaande redenering ook gebruiken voor deelruimten met dimensie groter dan $n-k$. Later bewijzen we in Stelling 3.1.1 dat voor een vast codewoord $c \in \mathcal{C}_k(n,q)$ het inproduct (c,ρ) een constante is voor alle deelruimten ρ met $\dim(\rho) \geq n-k$. Hieruit volgt ook dat het verschil van twee deelruimten die elk dimensie minstens $n-k$ hebben, een codewoord is van $\mathcal{C}_k(n,q)^\perp$.

We hebben nu een betere intuïtie over de codes $\mathcal{C}_k(n,q)$ en $\mathcal{C}_k(n,q)^\perp$. We kunnen ons afvragen wat er geweten is over de parameters van deze codes: de lengte, de dimensie en het minimum gewicht? Uit de definitie volgt er dat de lengte van de codes $\mathcal{C}_{j,k}(n,q)$ en $\mathcal{C}_{j,k}(n,q)^\perp$ gelijk is aan $\begin{bmatrix} n+1 \\ j+1 \end{bmatrix}_q$. Hamada heeft bewezen wat de dimensie is van de code $\mathcal{C}_k(n,q)$:

Stelling 2.1.4. *[18] De dimensie van de code $\mathcal{C}_k(n,q)$, met $q = p^h$, is*

$$\sum_{s_0} \cdots \sum_{s_{h-1}} \prod_{l=0}^{h-1} \sum_{i=0}^{L(s_{l+1},s_l)} (-1)^i \binom{k+1}{i} \binom{k + s_{l+1}p - s_l - ip}{k},$$

waarin $L(s_{l+1}, s_l) = \left\lfloor \frac{s_{l+1}p - s_l}{p} \right\rfloor$ *en* $s_h = s_0$. *De sommen worden genomen over alle getallen* s_l, $l \in \{0, \ldots, h-1\}$ *zodat*

$$k+1 \leq s_l \leq n+1 \text{ en } 0 \leq s_{l+1}p - s_l \leq (n+1)(p+1).$$

We aanvaarden deze stelling zonder bewijs. Ook voor $j > 0$ en $k = n-1$ is in [2] bewezen wat de dimensie is. Voor andere waarden van j en k is nog niet geweten wat de dimensie van $\mathcal{C}_{j,k}(n,q)$ is. De dimensie van de duale code $\mathcal{C}_k(n,q)^\perp$ is gelijk aan de lengte van deze code min de dimensie van $\mathcal{C}_k(n,q)$. Dus ook deze is gekend voor $j = 0$ of $k = n-1$. In het volgende hoofdstuk zullen wij het minimum gewicht bespreken. Het minimum gewicht is het kleinste niet-nul gewicht van een codewoord. Voor $j = 0$ bekijken we dit in detail. Als $j > 0$ vermelden we wat er geweten is. Eenmaal het minimum gewicht bepaald is, kan men proberen te bepalen wat het volgende gewicht van de code is. Zo kunnen we steeds verdergaan om te weten te komen wat alle gewichten zijn. Daarnaast willen we ook graag weten: wanneer een codewoord c gewicht $w(c)$ heeft, hoe ziet $\mathrm{supp}(c)$ er dan uit in $\mathrm{PG}(n,q)$? Het zal blijken dat men al veel codewoorden met een klein gewicht heeft kunnen karakteriseren. In Hoofdstuk 5 sluiten we zelf ook gewichten van de code $\mathcal{C}_k(n,q)^\perp$ uit voor specifieke waarden van k en q. De details hierover geven we later.

Om deze sectie te eindigen, vermelden we dat men op verschillende manieren naar een code kan kijken. We definiëren eerst wat een incidentiestructuur is.

Definitie 2.1.5 (Incidentiestructuur). Een incidentiestructuur is een koppel $(\mathcal{P}, \mathcal{B})$ waarbij $\mathcal{B}$ een (multi)verzameling is van deelverzamelingen van $\mathcal{P}$. De elementen van $\mathcal{P}$ en $\mathcal{B}$ noemen we respectievelijk punten en blokken.

We kunnen dan voor elk blok B een karakteristieke functie χ_B definiëren:

$$\chi_B : \mathcal{P} \to \{0,1\} : P \mapsto \begin{cases} 1 & \text{als } P \in B, \\ 0 & \text{anders.} \end{cases}$$

De vectorruimte die bestaat uit alle functies van $\mathcal{P}$ naar $\mathbb{F}_p$ noteren we als $\mathbb{F}_p^{\mathcal{P}}$. De deelruimte die hierin wordt opgespannen door de karakteristieke functies van $(\mathcal{P}, \mathcal{B})$ vormt een code. We noemen dit de code geassocieerd aan de incidentiestructuur $(\mathcal{P}, \mathcal{B})$. We hadden de code $\mathcal{C}_{j,k}(n,q)$ ook op deze manier kunnen definiëren. We kiezen $\mathcal{P}$ en $\mathcal{B}$ hiervoor respectievelijk als de verzameling van alle j- en k-ruimten in $\mathrm{PG}(n,q)$. De karakteristieke vector χ_τ komt overeen met de karakteristieke functie χ_τ voor elke k-ruimte τ. Vandaar dat het geen probleem is om hiervoor hetzelfde symbool te gebruiken. Wij werken steeds met de karakteristieke vector.

2.2. Meetkundige structuren

We definiëren nu enkele meetkundige structuren die we later nodig hebben. Daarnaast geven we ook voorbeelden en enkele relevante eigenschappen van deze structuren. We beginnen met de definitie van een spread en gaan dan over naar k-blokkerende verzamelingen.

Definitie 2.2.1 (Spread). Een spread van $\mathrm{PG}(n,q)$ is een partitie van de puntenverzameling in deelruimten met een vaste dimensie. Als we de dimensie k willen specificeren, spreken we van een k-spread.

Definitie 2.2.2 (k-Blokkerende verzameling). Een k-blokkerende verzameling $\mathcal{B}$ in $\mathrm{PG}(n,q)$ is een puntenverzameling die met elke $(n-k)$-ruimte minstens één punt gemeen heeft, met $k \in \{0,\ldots,n-1\}$.

Een k-blokkerende verzameling wordt soms een blokkerende verzameling ten opzichte van $(n-k)$-ruimten genoemd. Wanneer we spreken over blokkerende verzamelingen bedoelen we hiermee 1-blokkerende verzamelingen.

Definitie 2.2.3 (Essentieel punt). Het punt P is een essentieel punt van de k-blokkerende verzameling $\mathcal{B}$ in $\mathrm{PG}(n,q)$, als er een $(n-k)$-ruimte bestaat die enkel het punt P gemeen heeft met $\mathcal{B}$.

Merk op dat als we een essentieel P punt weglaten uit een k-blokkerende verzameling $\mathcal{B}$, dan is $\mathcal{B} \setminus \{P\}$ geen k-blokkerende verzameling meer. Dit brengt ons tot de volgende definitie:

Definitie 2.2.4 (Minimale k-blokkerende verzameling). Een k-blokkerende verzameling in $\mathrm{PG}(n,q)$ is minimaal als elk punt essentieel is.

We zeggen ook dat een k-blokkerende verzameling $\mathcal{B}$ klein is wanneer $|\mathcal{B}| < \frac{3(q^k+1)}{2}$. Laten we een voorbeeld geven van zo een verzameling.

Voorbeeld 2.2.5. Stel dat τ een k-ruimte is in $\mathrm{PG}(n,q)$. Elke $(n-k)$-ruimte heeft minstens één punt gemeen met τ wegens de identiteit van Grassmann. Bijgevolg vormen de punten van τ een k-blokkerende verzameling $\mathcal{B}$. Deze is minimaal, want we kunnen voor elk punt $P \in \tau$ een $(n-k)$-ruimte ρ construeren die enkel het punt P gemeen heeft met deze deelruimte τ. Ook is dit voor $q > 2$ een kleine k-blokkerende verzameling:

$$\begin{aligned} \theta_k = \frac{q^{k+1}-1}{q-1} &< \frac{3(q^k+1)}{2} \\ \iff 2q^{k+1} - 2 &< 3q^{k+1} - 3q^k + 3q - 3 \\ \iff 0 &< q^{k+1} - 3q^k + 3q - 1. \end{aligned}$$

Men kan nagaan dat dit polynoom positief is voor de toegelaten waarden van q en k.

Een triviale k-blokkerende verzameling is een k-blokkerende verzameling die een k-ruimte bevat. Later zullen we o.a. werken met lineaire k-blokkerende verzamelingen. Deze worden op een specifieke wijze geconstrueerd. In $\mathrm{PG}(n,q)$, met $q = p^h$, kunnen we elk punt via veldreductie laten overeenkomen met een $(h-1)$-ruimte van $\mathrm{PG}((n+1)h-1,p)$. Elke rechte uit $\mathrm{PG}(n,q)$ komt dan overeen met een $(2h-1)$-ruimte van $\mathrm{PG}((n+1)h-1,p)$. In het algemeen is een k-ruimte in $\mathrm{PG}(n,q)$ een $((k+1)h-1)$-ruimte in $\mathrm{PG}((n+1)h-1,p)$. Merk op dat de punten van $\mathrm{PG}(n,q)$ een $(h-1)$-spread vormen in $\mathrm{PG}((n+1)h-1,p)$. We noemen deze spread een Desarguesiaanse spread. We kunnen dan de volgende verzameling definiëren:

Definitie 2.2.6. Gegeven een Desarguesiaanse $(h-1)$-spread $\mathcal{D}$ in $\mathrm{PG}((n+1)h-1,p)$. We definiëren $\mathcal{B}(U)$ als de verzameling $\{\rho \in \mathcal{D} \mid U \cap \rho \neq \emptyset\}$, met U een deelverzameling van $\mathrm{PG}((n+1)h-1,p)$.

Als τ een hk-ruimte is van $\mathrm{PG}((n+1)h-1,p)$, dan definieert $\mathcal{B}(\tau)$ de lineaire k-blokkerende verzameling in $\mathrm{PG}(n,q)$. We tonen aan dat dit inderdaad een k-blokkerende verzameling is. Neem hiervoor een willekeurige $(n-k)$-ruimte σ. Dan correspondeert σ met een $((n-k+1)h-1)$-ruimte in $\mathrm{PG}((n+1)h-1,p)$. Dankzij de identiteit van Grassmann moet deze minstens een punt P gemeen hebben met τ. Dit punt P ligt dan in een zekere $(h-1)$-ruimte $\rho \in \mathcal{B}(\tau) \subseteq \mathcal{D}$.

Het punt Q in $\mathrm{PG}(n,q)$ waarmee ρ overeenkomt, ligt dan in de $(n-k)$-ruimte σ. Dus definieert $\mathcal{B}(\tau)$ een k-blokkerende verzameling. Zo'n type k-blokkerende verzamelingen noemen we lineaire k-blokkerende verzamelingen. Het is ook geweten dat dit voorbeeld een kleine minimale k-blokkerende verzameling is. Merk op dat we hierboven steeds de identiteit van Grassmann gebruikten om uit te leggen waarom twee deelruimten met voldoende grote dimensies snijden. In het vervolg zullen we minder formeel zijn en dit argument niet meer expliciet vermelden.

Blokkerende verzamelingen t.o.v. $(n-k)$-ruimten hebben enkele interessante eigenschappen die we later zullen gebruiken. Een Nederlandstalig bewijs van de eerste stelling staat in [43], de bachelorproef van de auteur. Voor het originele bewijs verwijzen we naar de referentie die hieronder bij de stelling staat. We zullen onderstaande stellingen aanvaarden zonder bewijs.

Stelling 2.2.7. *[10, Stelling 2] Zij $\mathcal{B}$ een k-blokkerende verzameling in $\mathrm{PG}(n,q)$, dan is $|\mathcal{B}| \geq \theta_k$. Als $|\mathcal{B}| = \theta_k$, dan is $\mathcal{B}$ een k-ruimte.*

Lemma 2.2.8. *[22, Lemma 9] Gegeven een minimale k-blokkerende verzameling $\mathcal{B}$ in $\mathrm{PG}(n,q)$, $n \geq 2$, $q = p^h$, met $p > 5$, die elke $(n-k)$-ruimte snijdt in $1 \pmod p$ punten. Als $\theta_k < |\mathcal{B}| < 2q^k$, dan geldt er: $|\mathcal{B}| < \frac{3(p^{hk}-p^{hk-1})}{2}$.*

Stelling 2.2.9. *[41, Theorem 2.7] Gegeven een minimale k-blokkerende verzameling $\mathcal{B}$ in $\mathrm{PG}(n,q)$, $q = p^h$, $p > 2$, en $|\mathcal{B}| < \frac{3(q^k+1)}{2}$, dan geldt er voor elke deelruimte die $\mathcal{B}$ snijdt dat deze snijdt in $1 \pmod p$ punten.*

Stelling 2.2.10. *[26, Theorem 3] Een k-blokkerende verzameling $\mathcal{B}$ met grootte kleiner dan $2q^k$ is op unieke wijze reduceerbaar tot een minimale k-blokkerende verzameling.*

We gaan nu over naar andere speciale soorten verzamelingen. We frissen eerst de definitie van een secant op.

Definitie 2.2.11 (Secant). Beschouw een puntenverzameling $\mathcal{V}$ in $\mathrm{PG}(n,q)$. We noemen een deelruimte een m-secant aan $\mathcal{V}$ als deze juist m punten van $\mathcal{V}$ bevat. Wanneer het duidelijk is over welke deelruimte we spreken, laten we de deelruimte weg. Bijvoorbeeld we gebruiken 3-secant in plaats van 3-secant vlak. Daarnaast gebruiken we het begrip secant voor een deelruimte die minstens twee punten van $\mathcal{V}$ bevat. Bijvoorbeeld het 3-secant vlak noemen we ook een secant vlak of gewoon secant.

Definitie 2.2.12 (Boog). In $\mathrm{PG}(2,q)$ is een boog $\mathcal{V}$ een verzameling van punten zodat er geen drie punten op een rechte liggen. Als $\mathcal{V}$ bestaat uit m punten, met $m \in \mathbb{N}$, spreken we over een m-boog.

Een speciale eigenschap van een boog in $\mathrm{PG}(2,q)$ is dat er steeds een rechte bestaat die disjunct is aan de boog.

Stelling 2.2.13. *Er bestaat steeds een rechte die disjunct is aan een boog in $\mathrm{PG}(2,q)$.*

Bewijs. Een boog $\mathcal{V}$ in $\mathrm{PG}(2,q)$ bevat hoogstens $q+2$ punten. Dit kan men inzien door de rechten te bekijken door een punt P van de boog. Elke rechte door P kan hoogstens één extra punt bijdragen tot $\mathcal{V}$ per definitie. Zo vinden we dat als de boog $\mathcal{V}$ een m-boog is, dan is $m \leq q+2$. Men kan ook nog verder aantonen dat als $m = q+2$, dan moet q even zijn. Elke rechte snijdt $\mathcal{V}$ in twee, één of nul punten. Het aantal 2-secanten is gelijk aan $\binom{m}{2} = \frac{m(m-1)}{2}$. De rechten door een vast punt $P \in \mathcal{V}$ zijn ofwel 2-secanten ofwel raaklijnen. Aangezien er door P juist $m-1$ verschillende 2-secanten zijn, is het aantal raaklijnen door P gelijk aan $q+1-(m-1)$. In totaal zijn er bijgevolg $m(q+2-m)$ raaklijnen aan de m-boog. Dit betekent dat het aantal verschillende rechten die de m-boog snijden gelijk is aan

$$\begin{aligned} f(m) &= \frac{m(m-1)}{2} + m(q+2-m) = m\left(\frac{m-1}{2} + q + 2 - m\right) \\ &= m\frac{2q+3-m}{2} = \frac{2qm+3m-m^2}{2}. \end{aligned}$$

Dit aantal is maximaal als $f'(m) = \frac{2q+3-2m}{2} = 0$, m.a.w. als $m = q+\frac{3}{2}$. We zullen dus het meeste aantal rechten snijden als $m = q+1$ of $m = q+2$. In deze gevallen vinden we $f(q+1) = \frac{(q+1)(q+2)}{2} = f(q+2)$. In het bijzonder is dit strikt kleiner dan θ_2, wat het totale aantal rechten is. We vinden dus dat er inderdaad steeds een rechte bestaat die disjunct is aan een boog. ■

Bij de volgende verzameling geeft de naam al een hint naar de betekenis.

Definitie 2.2.14 (Even verzameling). Een even verzameling in $\mathrm{PG}(n,q)$, met q even, is een verzameling $\mathcal{V}$ bestaande uit punten zodat elke rechte een even aantal punten bevat van $\mathcal{V}$.

In het bijzonder mag een rechte dus ook nul punten van een even verzameling bevatten. Analoog kan men ook een oneven verzameling definiëren als een puntenverzameling zodat elke rechte een oneven aantal punten ervan bevat. We bewijzen dat elke even verzameling een even grootte heeft.

Lemma 2.2.15. *Stel dat $\mathcal{V}$ een even verzameling is in $\mathrm{PG}(n,q)$, met q even, dan is $|\mathcal{V}|$ even.*

Bewijs. Als $\mathcal{V}$ de ledige verzameling is, is de stelling duidelijk waar. Stel dat $\mathcal{V}$ minstens één punt P bevat. Het punt P ligt op θ_{n-1} verschillende rechten. Al deze rechten door P bevatten naast het punt P een oneven aantal punten van $\mathcal{V}$. We noteren dit aantal extra punten van $\mathcal{V}$ in de rechte l_i door P als x_i, met $i \in \{1,\ldots,\theta_{n-1}\}$. We vinden dat $|\mathcal{V}| = 1 + \sum_{i=1}^{\theta_{n-1}} x_i$. Een som die bestaat uit een oneven aantal termen waarin elke term oneven is, is zelf oneven. Omdat q even is, is θ_{n-1} oneven. Uit bovenstaande gelijkheid volgt dus dat $|\mathcal{V}|$ even is. ■

We geven ook een voorbeeld van een even verzameling in het vlak $\mathrm{PG}(2,q)$.

Voorbeeld 2.2.16. In $\mathrm{PG}(2,q)$, met q even, is een hyperovaal, i.e. een verzameling van punten die elke rechte snijdt in nul of twee punten, een voorbeeld van een even verzameling. Een gekende hyperovaal is een irreducibele kegelsnede met zijn kern. Elke hyperovaal die van deze vorm is, noemen we een reguliere hyperovaal. Merk op dat dit ook een voorbeeld is van een $(q+2)$-boog.

We bespreken tot slot nog een laatste begrip.

Definitie 2.2.17 (Quotiëntmeetkunde). Neem een $(n-k-1)$-ruimte ρ van $\mathrm{PG}(n,q)$, met $k \in \{0,\ldots,n-1\}$. We definiëren nu de quotiëntmeetkunde $\mathrm{PG}(n,q)/\rho$. Dit is een projectieve ruimte van dimensie k waarin elke i-ruimte van $\mathrm{PG}(n,q)/\rho$ overeenkomt met een $(n-k+i)$-ruimte van $\mathrm{PG}(n,q)$ die ρ bevat. Ook blijft incidentie bewaard. Bijvoorbeeld de $(n-k)$-ruimten die ρ bevatten, zijn de punten van $\mathrm{PG}(n,q)/\rho$.

Nu we al deze begrippen hebben opgefrist, kunnen we beginnen met het bestuderen van $\mathcal{C}_k(n, q)$ en $\mathcal{C}_k(n, q)^{\perp}$. Het volgende hoofdstuk onderzoekt het minimum gewicht van deze codes. Indien we weten wat dit is, bespreken we hoe de minimum gewicht codewoorden eruit zien.

3 Minimum gewicht

3.1. Verband met blokkerende verzamelingen

In dit hoofdstuk bestuderen we het minimum gewicht van de codes $\mathcal{C}_k(n,q)$ en $C_k(n,q)^\perp$. Voor de eerste code zullen we het minimum gewicht kunnen bepalen, voor de tweede code kunnen we het minimum gewicht in de meeste situaties enkel begrenzen. Voor we beginnen met het bespreken van het minimum gewicht tonen we in deze sectie eerst enkele belangrijke eigenschappen en verbanden aan. Deze geven ons al wat meer inzicht in de structuur van de codes. De eerste stelling is een uitbreiding van [26, Lemma 2].

Stelling 3.1.1. *Voor elk codewoord $c \in \mathcal{C}_k(n,q)$ bestaat er een constante b, $b \in \mathbb{F}_p$, zodat voor elke deelruimte ρ met $\dim(\rho) \geq n-k$, geldt dat $(c,\rho) = b$. Meer specifiek is b de som van de coëfficiënten van het codewoord c.*

Bewijs. We geven hier een bewijs dat een uitbreiding is van het bewijs van [1, Lemma 4.3]. Neem een codewoord $c \in \mathcal{C}_k(n,q)$ en een willekeurige deelruimte ρ die minstens dimensie $n-k$ heeft. Per definitie is $c = \sum_i a_i \chi_{\tau_i}$ met τ_i verschillende k-ruimten en $a_i \in \mathbb{F}_p$. Een deelruimte waarvan de dimensie minstens $n-k$ is, en een k-ruimte snijden altijd in $\mathrm{PG}(n,q)$, dus is $|\rho \cap \tau_i| = 1 \pmod p$. We vinden dat:

$$(c,\rho) = \left(\sum_i a_i \chi_{\tau_i}\right) \chi_\rho = \sum_i a_i (\chi_{\tau_i}\chi_\rho) = \sum_i a_i = b.$$

Merk op dat de constante b inderdaad de som van de coëfficiënten is van het codewoord c. ∎

Gevolg 3.1.2. *[22] Gegeven een codewoord $c \in \mathcal{C}_k(n,q)$, als er een $(n-k)$-ruimte ρ bestaat zodat $(c,\rho) = 0$, dan geldt er dat $c \in \mathcal{C}_{n-k}(n,q)^\perp$.*

Bewijs. Dankzij de vorige stelling weten we dat dan voor alle $(n-k)$-ruimten τ geldt $(c,\tau) = b = 0$. Uit het feit dat $\mathcal{C}_{n-k}(n,q)$ wordt voortgebracht door alle $(n-k)$-ruimten, volgt dan dat $c \in \mathcal{C}_{n-k}(n,q)^\perp$. ∎

We geven hier nog een andere eigenschap die volgt uit Stelling 3.1.1. We zullen deze later gebruiken.

Gevolg 3.1.3. *[26, Lemma 3] Als $k \geq \frac{n}{2}$, dan is een codewoord $c \in \mathcal{C}_k(n,q)$ bevat in $\mathcal{C}_k(n,q) \cap \mathcal{C}_k(n,q)^\perp$ als en slechts als $(c,\rho) = 0$ voor alle deelruimten ρ met $\dim(\rho) \geq n-k$.*

Bewijs. Stel dat $c \in \mathcal{C}_k(n,q) \cap \mathcal{C}_k(n,q)^\perp$. In het bijzonder is $c \in \mathcal{C}_k(n,q)^\perp$, dus is $(c,\rho) = 0$ voor alle k-ruimten ρ. Omdat $k \geq \frac{n}{2}$, is $k \geq n-k$, dus volgt uit Stelling 3.1.1 dat $(c,\rho) = 0$ voor alle deelruimten ρ met $\dim(\rho) \geq n-k$.

Omgekeerd stel dat $(c,\rho) = 0$ voor alle deelruimten ρ met $\dim(\rho) \geq n-k$. Aangezien $k \geq n-k$, geldt er dus specifiek voor de k-ruimten ρ dat $(c,\rho) = 0$. Er volgt dat $c \in \mathcal{C}_k(n,q)^\perp$, omdat de k-ruimten de code $\mathcal{C}_k(n,q)$ voortbrengen. ∎

De volgende stelling zullen we ook vaak kunnen gebruiken.

Stelling 3.1.4. *Beschouw een niet-nul codewoord $c \in \mathcal{C}_k(n,q)$ dat met elke $(n-k)$-ruimte minstens één punt gemeen heeft en $w(c) \leq 2q^k$. Dan bestaat er een punt $R \in \mathrm{supp(c)}$ en een $(n-k)$-ruimte ρ zodat $\rho \cap \mathrm{supp}(c) = \{R\}$. Als c een niet-nul codewoord is van $\mathcal{C}_k(n,q)$ of van $\mathcal{C}_{n-k}(n,q)^\perp$ met $w(c) \leq 2q^k$, dan bestaat er voor elk punt $P \in \mathrm{supp(c)}$ een $(n-k-1)$-ruimte die raakt aan $\mathrm{supp}(c)$ in het punt P.*

Bewijs. Beschouw een codewoord c zoals in het gegeven en we noteren $\mathrm{supp}(c)$ als $\mathcal{S}$. Het bewijs dat we geven, is gebaseerd op een deel van het bewijs van [26, Theorem 4]. We tonen eerst aan dat er een punt $R \in \mathcal{S}$ bestaat dat in een $(n-k)$-ruimte ligt die raakt aan $\mathcal{S}$. Uit het gegeven volgt er dat $\mathcal{S}$ met elke $(n-k)$-ruimte een punt gemeen heeft. Stel dat elke $(n-k)$-ruimte minstens twee punten van $\mathcal{S}$ bevat. We tellen de koppels (P,τ), met $P \in \mathcal{S}$ en τ een $(n-k)$-ruimte door P, op twee manieren. Voor P hebben we $|\mathcal{S}|$ mogelijkheden en door elk punt P zijn er $\begin{bmatrix} n \\ n-k \end{bmatrix}_q$ verschillende $(n-k)$-ruimten. Langs de andere kant weten we dat er $\begin{bmatrix} n+1 \\ n-k+1 \end{bmatrix}_q$ verschillende $(n-k)$-ruimten zijn in $\mathrm{PG}(n,q)$ die elk minstens twee punten van $\mathcal{S}$ bevatten per veronderstelling. Dit geeft de volgende ongelijkheid:

$$|\mathcal{S}| \begin{bmatrix} n \\ n-k \end{bmatrix}_q \geq 2 \begin{bmatrix} n+1 \\ n-k+1 \end{bmatrix}_q,$$

als we hierin ook gebruiken dat $|\mathcal{S}| \leq 2q^k$ vinden we dat:

$$\begin{aligned} & 2q^k \begin{bmatrix} n \\ n-k \end{bmatrix}_q \geq 2 \begin{bmatrix} n+1 \\ n-k+1 \end{bmatrix}_q \\ \iff & q^k \geq \frac{(q^{n+1}-1)\cdot\ldots\cdot(q^{k+1}-1)}{(q^{n-k+1}-1)\cdot\ldots\cdot(q-1)} \frac{(q^{n-k}-1)\cdot\ldots\cdot(q-1)}{(q^n-1)\cdot\ldots\cdot(q^{k+1}-1)} = \frac{(q^{n+1}-1)}{(q^{n-k+1}-1)} \\ \iff & q^{n+1} - q^k \geq q^{n+1} - 1. \end{aligned}$$

Dit geeft een contradictie aangezien $q \geq 2$ en $k > 0$. We hebben dus bewezen dat er een punt $R \in \mathcal{S}$ bestaat waardoor er een raak $(n-k)$-ruimte τ aan $\mathcal{S}$ bestaat.

We bewijzen nu het tweede deel van de stelling, neem hiervoor een willekeurig punt $P \in \mathcal{S}$. Als $k = n-1$, dan is de stelling bewezen omdat het punt P zelf de gezochte deelruimte is. Veronderstel nu dat $1 \leq k \leq n-2$. Uit het feit dat $|\mathcal{S}| \leq 2q^k$ en dat er θ_{n-1} rechten zijn door het punt P volgt dat er een rechte bestaat die raakt aan $\mathcal{S}$ in P. We kunnen dit argument inductief blijven herhalen tot we vinden dat er een $(n-k-2)$-ruimte bestaat door P die raakt aan $\mathcal{S}$. Hierdoor zijn er θ_{k+1} verschillende $(n-k-1)$-ruimten. Omdat $|\mathcal{S}| \leq 2q^k$ en $2q^k \leq \theta_{k+1}$, vinden we een $(n-k-1)$-ruimte τ door P die raakt aan $\mathcal{S}$. ∎

Dankzij Stellingen 3.1.1 en 3.1.4 kunnen we in de volgende stelling aantonen dat bepaalde codewoorden c van $\mathcal{C}_k(n,q)$ met een voldoende klein gewicht een minimale k-blokkerende verzameling vormen. Dit verband zal later belangrijk zijn om het bestaan van sommige codewoorden te kunnen uitsluiten.

Stelling 3.1.5. *[26, Theorem 4] Voor een codewoord $c \in \mathcal{C}_k(n,q)$ met gewicht kleiner dan $2q^k$ geldt dat als er een $(n-k)$-ruimte ρ bestaat zodat $(c,\rho) \neq 0$, dan is $\mathrm{supp}(c)$ een minimale k-blokkerende verzameling in $\mathrm{PG}(n,q)$. Ook behoren de coëfficiënten van c tot de verzameling $\{0,a\}$, met $a \in \mathbb{F}_p^*$, en heeft $\mathrm{supp}(c)$ met elke $(n-k)$-ruimte $1 \pmod p$ punten gemeen.*

Bewijs. Wegens Stelling 3.1.1 weten we dat als $(c, \rho) = a \neq 0$ is voor één $(n-k)$-ruimte ρ, dan is dit waar voor alle $(n-k)$-ruimten. In het bijzonder moet de verzameling $\mathrm{supp}(c)$, die we zullen noteren als $\mathcal{S}$, met elke $(n-k)$-ruimte minstens één punt gemeenschappelijk hebben. Bijgevolg is $\mathcal{S}$ een k-blokkerende verzameling. Dankzij Stelling 3.1.4 bestaat er een punt $R \in \mathcal{S}$ dat in een $(n-k)$-ruimte τ ligt die raakt aan $\mathcal{S}$. Aangezien $(c, \tau) = a$ is $c_R = a$. Merk op dat dit geldt voor elk essentieel punt van de blokkerende verzameling $\mathcal{S}$. We bewijzen nu dat $\mathcal{S}$ minimaal is. Veronderstel hiervoor dat $\mathcal{S}$ een punt Q bevat dat niet essentieel is. Uit Stelling 3.1.4 weten we dat er een $(n-k-1)$-ruimte σ bestaat die enkel het punt Q gemeen heeft met $\mathcal{S}$. Merk op dat als $k = n-1$, dit het punt Q zelf is. Als elke $(n-k)$-ruimte door σ, dit zijn er θ_k, twee extra punten van $\mathcal{S}$ zou bevatten, hebben we dat:

$$2q^k \geq |\mathcal{S}| \geq 1 + 2\theta_k,$$

wat een strijdigheid geeft. Er bestaat dus een $(n-k)$-ruimte σ die enkel het punt Q en een ander punt Q' van $\mathcal{S}$ bevat. We weten dat $(c, \sigma) = c_Q + c_{Q'} = a$ en uit Lemma 2.2.10 volgt er dat we $\mathcal{S}$ op unieke manier kunnen reduceren naar een minimale k-blokkerende verzameling. Bijgevolg is Q' een essentieel punt. Immers als dit niet zo is kunnen we zowel Q als Q' verwijderen en is de overblijvende verzameling nog steeds een k-blokkerende verzameling. Echter heeft deze geen punt gemeen met σ, wat een strijdigheid geeft. Dus is Q' een essentieel punt en is $c_{Q'} = a$. Hierdoor moet c_Q gelijk zijn aan nul opdat $(c, \sigma) = c_Q + c_{Q'} = a$. Dit kan echter niet, want $Q \in \mathcal{S}$, dus bevat $\mathcal{S}$ geen niet essentiële punten en is het een minimale k-blokkerende verzameling. Aangezien elk punt essentieel is, heeft elk punt van $\mathcal{S}$ als coördinaat a. Echter is ook $(c, \rho) = a$ voor elke $(n-k)$-ruimte ρ, dus moet $|\mathcal{S} \cap \rho| = 1 \mod p$. ■

3.2. Minimum gewicht van de incidentiecode

We bewijzen nu wat het minimum gewicht is van de code $\mathcal{C}_k(n, q)$ en hoe deze codewoorden eruit zien. Hiervoor volgen we de aanpak van Bagchi en Inamdar uit [8]. We definiëren eerst een projectie afbeelding.

Definitie 3.2.1 (Projectie afbeelding [8]). Gegeven een k-ruimte ρ en een disjuncte $(n-k-1)$-ruimte σ in $\mathrm{PG}(n, q)$. We definiëren de projectie afbeelding $p : \mathrm{PG}(n, q) \setminus \rho \to \sigma$ zodat die elk punt $P \in \mathrm{PG}(n, q) \setminus \rho$ afbeeldt op het unieke punt $\langle P, \rho \rangle \cap \sigma$.

Merk op dat deze afbeelding goed gedefinieerd is net omdat σ en ρ disjunct zijn, maar elke uitbreiding van ρ de deelruimte σ wel zal snijden door de keuzes van de dimensies. Deze projectie afbeelding zullen we gebruiken om eerst volgend lemma aan te tonen. Nadien bewijzen we de karakterisering van de minimum codewoorden van $\mathcal{C}_k(n, q)$.

Lemma 3.2.2. *[8, Corollary 1] Gegeven een verzameling $\mathcal{A}$ bestaande uit s-ruimten van $\mathrm{PG}(n, q)$ met $|\mathcal{A}| \leq \theta_{n-k}$ en $0 \leq s \leq k \leq n$. Voor elke s-ruimte $\rho \in \mathcal{A}$ bestaat er dan een k-ruimte τ zodat ρ de enige deelruimte van $\mathcal{A}$ is die bevat is in τ.*

Bewijs. Neem een s-ruimte ρ uit de verzameling $\mathcal{A}$. Kies vervolgens een $(n-s-1)$-ruimte σ die disjunct is aan ρ en beschouw de projectie $p : \mathrm{PG}(n, q) \setminus \rho \to \sigma$. Voor elke s-ruimte ρ' van $\mathcal{A}$, met $\rho' \neq \rho$, kiezen we een punt $R \in \rho' \setminus \rho$. De puntenverzameling bestaande uit de projecties van deze punten noemen we $\mathcal{A}'$. In het bijzonder is $|\mathcal{A}'| < \theta_{n-k}$ omdat we geen punt hebben gekozen voor ρ. We definiëren $N = n - s - 1$, dan is $\mathcal{A}'$ een puntenverzameling in $\mathrm{PG}(N, q)$ en $|\mathcal{A}'| < \theta_{N+s+1-k}$. Uit Stelling 2.2.7 over blokkerende verzamelingen volgt dat er een $(k-s-1)$-ruimte τ' bestaat

die geen enkel punt gemeen heeft met $\mathcal{A}'$. De deelruimte $\tau = \langle \rho, \tau' \rangle$ heeft dimensie k en is de gezochte deelruimte. Immers elke andere deelruimte van $\mathcal{A}$ kan niet bevat zijn in τ, want dan zou het bijhorende gekozen punt R liggen in τ. Bij definitie volgt er dan dat $p(R) \in \tau'$, wat niet kan omdat $\mathcal{A}' \cap \tau' = \emptyset$. We kunnen dus besluiten dat τ enkel de deelruimte ρ van $\mathcal{A}$ bevat en dat de stelling bewezen is. ■

Stelling 3.2.3. *[8, Proposition 1] Het minimum gewicht van $\mathcal{C}_k(n,q)$ is θ_k en de codewoorden van minimum gewicht zijn de scalaire veelvouden van de k-ruimten.*

Bewijs. We weten vanuit Hoofdstuk 2 dat er codewoorden zijn met gewicht θ_k, namelijk de incidentievectoren van de k-ruimten die de code $\mathcal{C}_k(n,q)$ voortbrengen. Veronderstel dus dat $c \in \mathcal{C}_k(n,q)$ een codewoord is met $w(c) \leq \theta_k$. We kunnen bovenstaand lemma toepassen op $\text{supp}(c) = \mathcal{S}$ met $s = 0$ zodat we een $(n-k)$-ruimte τ vinden die $\mathcal{S}$ snijdt in juist één punt. We weten dan uit Stelling 3.1.1 dat elke $(n-k)$-ruimte minstens één punt gemeen heeft met $\mathcal{S}$. Hieruit volgt dat $\mathcal{S}$ een k-blokkerende verzameling is met hoogstens grootte θ_k. Dankzij Stelling 2.2.7 is $\mathcal{S}$ hierdoor een k-ruimte. Merk nu op dat twee codewoorden met minimum gewicht waarvan de supports samenvallen scalaire veelvouden van elkaar moeten zijn. Anders zou er een lineaire combinatie bestaan van deze codewoorden met een strikt kleiner gewicht, wat een strijdigheid geeft. Hierdoor en door het feit dat de incidentievectoren codewoorden zijn, volgt er dat alle codewoorden van minimum gewicht scalaire veelvouden zijn van de incidentievectoren van k-ruimten. ■

Hiermee hebben we de codewoorden van minimum gewicht van $\mathcal{C}_k(n,q)$ geclassificeerd. In het geval dat $k = n-1$, bepalen we vervolgens het minimum gewicht van $\mathcal{C}_k(n,q) \cap \mathcal{C}_k(n,q)^\perp$.

3.2.1. Doorsnede van de code van punten en hypervlakken en zijn duale code

In dit deel bespreken we kort het minimum gewicht van $\mathcal{C}_{n-1}(n,q) \cap \mathcal{C}_{n-1}(n,q)^\perp$, want we zullen dit later nog gebruiken om codewoorden uit te sluiten. We aanvaarden onderstaande stelling die aantoont wat het minimum gewicht is van $\mathcal{C}_1(2,q) \cap \mathcal{C}_1(2,q)^\perp$. Voor het bewijs verwijzen we de geïnteresseerde lezer naar [7, Corollary 6.4.4] van Assmus en Key. In de stelling daarna tonen we zoals Lavrauw, Storme en Van de Voorde in [25, Theorem 5] aan hoe we dit gegeven kunnen gebruiken om het minimum gewicht van $\mathcal{C}_{n-1}(n,q) \cap \mathcal{C}_{n-1}(n,q)^\perp$ te bepalen voor grotere n.

Stelling 3.2.4. *[7, Corollary 6.4.4] In $\mathcal{C}_1(2,q) \cap \mathcal{C}_1(2,q)^\perp$ zijn de codewoorden met minimum gewicht de scalaire veelvouden van het verschil van de incidentievectoren van twee verschillende rechten. Hierdoor is het minimum gewicht $2q$.*

Stelling 3.2.5. *[25, Theorem 5] Het minimum gewicht van $\mathcal{C}_{n-1}(n,q) \cap \mathcal{C}_{n-1}(n,q)^\perp$ is $2q^{n-1}$.*

Bewijs. Er volgt uit Hoofdstuk 2 dat het verschil van de incidentievectoren van twee hypervlakken een codewoord van $\mathcal{C}_{n-1}(n,q) \cap \mathcal{C}_{n-1}(n,q)^\perp$ met gewicht $2q^{n-1}$. Het is dus voldoende om aan te tonen dat er geen codewoorden bestaan met een kleiner gewicht. We bewijzen dit vanuit het ongerijmde. Stel dat $c \in \mathcal{C}_{n-1}(n,q) \cap \mathcal{C}_{n-1}(n,q)^\perp$ een niet-nul codewoord is zodat $w(c) < 2q^{n-1}$. Het idee van het bewijs is dat we de situatie zullen herleiden naar het geval $n = 2$, waar we weten wat het minimum gewicht is. Aangezien $n - 1 \geq \frac{n}{2}$, kunnen we Stelling 3.1.3 toepassen op $\mathcal{C}_{n-1}(n,q) \cap \mathcal{C}_{n-1}(n,q)^\perp$. Deze zegt dat een codewoord $c' \in \mathcal{C}_{n-1}(n,q)$ ook bevat is in $\mathcal{C}_{n-1}(n,q)^\perp$ als en slechts als $(c', \rho) = 0$ voor alle deelruimten ρ met $\dim(\rho) \geq 1$. Hieruit volgt dat in het bijzonder elke rechte nul of minstens twee punten bevat van $\text{supp}(c) = \mathcal{S}$. We tonen aan dat er een rechte l bestaat die exact twee punten van $\mathcal{S}$ bevat. Neem hiervoor een punt $P \in \mathcal{S}$. Door P zijn er θ_{n-1} rechten in $\text{PG}(n,q)$. Als al deze rechten minstens twee extra punten van $\mathcal{S}$ bevatten,

dan zou $w(c) \geq 1 + 2\theta_{n-1}$, wat niet kan. Beschouw dus inderdaad een rechte l die exact twee punten gemeen heeft met $\mathcal{S}$. We bekijken de vlakken π door l. Wanneer we de restrictie van c tot π nemen, zien we dat dit een codewoord is van de code $\mathcal{C}_1(\pi)$. Inderdaad c is een lineaire combinatie van hypervlakken en een hypervlak snijdt π ofwel in een rechte ofwel is π bevat in dit hypervlak. In dit laatste geval kunnen we de restrictie van het hypervlak tot π omschrijven als een bundel van rechten bestaande uit alle rechten door een vast punt P. Inderdaad het punt P komt dan $q + 1 = 1 \pmod p$ keer voor. Alle andere punten komen juist één keer voor. We vinden dus voor elk punt van π dat het coëfficiënt één heeft en dat de beschrijving via de rechten door P klopt. We kunnen dus steeds $c|_\pi$ schrijven als een lineaire combinatie van rechten in π. Dit betekent dat de beperking van c tot π een codewoord is van $\mathcal{C}_1(\pi)$. Daarnaast is dankzij Stelling 3.1.3 het codewoord $c|_\pi$ ook bevat in $\mathcal{C}_1(\pi)^\perp$, omdat voor elke rechte $m \in \pi$ geldt dat $(c, m) = 0$. We weten ook dat $c|_\pi$ niet het nulcodewoord is, want $l \subset \pi$ en $l \cap \mathcal{S} \neq \emptyset$. Uit Stelling 3.2.4 volgt er dat $w\left(c|_\pi\right) \geq 2q$. Aangezien er θ_{n-2} vlakken zijn door de rechte l en $|l \cap \mathcal{S}| = 2$, besluiten we dat $w(c) \geq (2q-2)\theta_{n-2} + 2 = 2(\theta_{n-1} - 1 - \theta_{n-2}) + 2 = 2q^{n-1}$. Dit geeft een strijdigheid met de assumptie dat $w(c) < 2q^{n-1}$ en we hebben de stelling dus bewezen. ■

In [34] hebben Polverino en Zullo bewezen dat de codewoorden van $\mathcal{C}_{n-1}(n, q)$ met gewicht $2q^{n-1}$ scalaire veelvouden zijn van het verschil van twee verschillende hypervlakken. Hieruit volgt dat de minimum gewicht codewoorden van $\mathcal{C}_{n-1}(n, q) \cap \mathcal{C}_{n-1}(n, q)^\perp$ ook scalaire veelvouden zijn van het verschil van de karakteristieke vectoren van twee verschillende hypervlakken.

3.3. Ondergrens voor het minimum gewicht van de duale code

3.3.1. Ondergrens via tellingen

Uit Hoofdstuk 2 weten we dat het verschil van twee verschillende $(n-k)$-ruimten die snijden in een $(n-k-1)$-ruimte een codewoord is van $\mathcal{C}_k(n, q)^\perp$ met gewicht $2q^{n-k}$. We kunnen ons nu afvragen of er kleinere codewoorden bestaan. In dit deel bewijzen we verschillende ondergrenzen voor het minimum gewicht van $\mathcal{C}_k(n, q)^\perp$. Als q priem of even is, zullen we het minimum gewicht exact kunnen bepalen. Tenslotte zullen we de verschillende ondergrenzen met elkaar vergelijken. In deze subsectie bepalen we de eerste ondergrens, deze vooral steunt op het maken van de juiste tellingen. We doen dit zoals Lavrauw, Storme en Van de Voorde in [26]. We bewijzen eerst een lemma voor we de ondergrens bewijzen.

Lemma 3.3.1. *[26, lemma 13] Stel dat q oneven is en dat er $2m$ verschillende niet-nul symbolen gebruikt zijn in het codewoord $c \in \mathcal{C}_k(n, q)^\perp$ en dat $w(c) \leq 2q^{n-k}$, dan is*

$$w(c) \geq \frac{4m}{2m+1}\theta_{n-k} + \frac{2m}{2m+1}.$$

Bewijs. Beschouw een codewoord $c \in \mathcal{C}_k(n, q)^\perp$ met $w(c) \leq 2q^{n-k}$. We noteren $w(c)$ als $\theta_{n-k} + x$ en $\mathrm{supp}(c)$ als $\mathcal{S}$. Uit Stelling 3.1.4 weten we dat er door elk punt $P \in \mathcal{S}$ een $(k-1)$-ruimte ρ' bestaat die raakt aan $\mathcal{S}$ in P. We noemen een k-ruimte die exact twee punten van $\mathcal{S}$ bevat een 2-secant om de notatie te vereenvoudigen. Het aantal 2-secanten door een $(k-1)$-ruimte die enkel het punt P van $\mathcal{S}$ bevat, noteren we als X_P. Omdat $(c, \tau) = 0$ voor elke k-ruimte τ, hebben we in het bijzonder dat als τ een 2-secant is door de punten P en Q dat $c_P = -c_Q$. Dit wil zeggen dat de coëfficiënt c_P minstens X_Q keer voorkomt. Omdat q oneven is, volgt er ook dat het aantal gebruikte symbolen even moet zijn. We noteren dit aantal als $2m$. Beschouw een $(k-1)$-ruimte ρ, zodat $\rho \cap \mathcal{S}$ juist één punt bevat en waarvoor het aantal 2-secanten dat door ρ gaat minimaal is.

Laat R het enige punt van $\mathcal{S}$ in ρ zijn. Alle gebruikte symbolen in het codewoord c komen minstens X_R keer voor door de minimaliteit van het aantal 2-secanten door ρ. Dit kunnen we gebruiken om een ondergrens te bepalen voor $w(c)$. In totaal zijn er θ_{n-k} verschillende k-ruimten τ door ρ in $\mathrm{PG}(n,q)$ en deze moeten allemaal minstens nog één extra punt van $\mathcal{S}$ bevatten opdat $(c,\tau)=0$. Naast R zijn er nog $\theta_{n-k}+x-1$ andere punten in $\mathcal{S}$. Uit het duivenhokprincipe volgt er dat er dan minstens $\theta_{n-k}-x+1$ verschillende k-ruimten zijn door ρ die exact één extra punt bevatten. Hieruit volgt dat $X_R \geq \theta_{n-k}-x+1$ en omdat elk symbool, dit zijn er $2m$, minstens evenveel gebruikt wordt als X_R hebben we wat wilden bewijzen:

$$\begin{aligned}
&2m(\theta_{n-k}-x+1) \leq \theta_{n-k}+x = |\mathcal{S}| \\
\iff &(2m-1)\theta_{n-k}+2m \leq (2m+1)x \\
\iff &\frac{2m-1}{2m+1}\theta_{n-k}+\frac{2m}{2m+1} \leq x \\
\iff &\frac{2m-1}{2m+1}\theta_{n-k}+\frac{2m}{2m+1} \leq w(c)-\theta_{n-k} \\
\iff &\frac{4m}{2m+1}\theta_{n-k}+\frac{2m}{2m+1} \leq w(c).
\end{aligned}$$

■

Via dit lemma kunnen we nu op eenvoudige wijze een ondergrens bepalen.

Stelling 3.3.2. *[26, Theorem 14] Voor $p \neq 2$ is het minimum gewicht van $\mathcal{C}_k(n,q)^\perp$ minstens $\frac{4\theta_{n-k}+2}{3}$.*

Bewijs. We bewijzen de stelling vanuit het ongerijmde. Stel dat $c \in \mathcal{C}_k(n,q)^\perp$ en $w(c) < \frac{4\theta_{n-k}+2}{3}$. Dankzij Stelling 3.1.4 bestaat er een $(k-1)$-ruimte ρ die juist één punt P van $\mathrm{supp}(c)$ bevat. Bij definitie van de code $\mathcal{C}_k(n,q)^\perp$ moet elke k-ruimte τ door ρ voldoen aan $(c,\tau)=0$. Uit Lemma 3.3.1 volgt dat c maar één symbool gebruikt. Daardoor moet τ minstens $p-1$ extra punten van $\mathrm{supp}(c)$ bevatten opdat $(c,\tau)=0$. Daarnaast zijn er θ_{n-k} verschillende mogelijkheden voor τ. Hierdoor is $w(c) \geq 1+(p-1)\theta_{n-k}$, wat de beloofde strijdigheid geeft. ■

Echter als $p \geq 7$ kunnen we bovenstaand Lemma 3.3.1 gebruiken om een betere ondergrens te bepalen.

Stelling 3.3.3. *[26, Theorem 15] Als $p=7$, dan is het minimum gewicht van $\mathcal{C}_k(n,q)^\perp$ minstens $\frac{12\theta_{n-k}+2}{7}$. Als $p>7$, dan is het minimum gewicht minstens $\frac{12\theta_{n-k}+6}{7}$.*

Bewijs. Stel dat $c \in \mathcal{C}_k(n,q)^\perp$ een codewoord is met minimum gewicht. We weten al dat $w(c) \leq 2q^{n-k}$. We veronderstellen dat $w(c) < \frac{12\theta_{n-k}+2}{7}$ als $p=7$ en $w(c) < \frac{12\theta_{n-k}+6}{7}$ als $p>7$. De ondergrens die we willen bewijzen is voor $p>7$ sterker dan voor $p=7$. Wanneer we later op zoek gaan naar een strijdigheid is het dus toegelaten om enkel de conditie $w(c) < \frac{12\theta_{n-k}+6}{7}$ te verifiëren. Aangezien $q=p^h$ oneven is, volgt er uit Lemma 3.3.1 dat er hoogstens vier niet-nul symbolen gebruikt zijn in het codewoord c, want bij zes niet-nul symbolen zou $w(c) \geq \frac{12\theta_{n-k}+6}{7}$, wat niet kan door onze aanname. We bespreken eerst het geval waarin er twee niet-nul symbolen zijn, en tonen aan dat dit niet mogelijk is. Nadien doen we hetzelfde voor vier niet-nul symbolen. Dit geeft aanleiding tot een strijdigheid en dus hebben we dan de stelling bewezen. Merk op dat we zullen gebruiken dat als a een coëfficiënt is, dan is ook $-a$ een coëfficiënt zoals we in het bewijs van de vorige stelling hebben afgeleid.

Geval 1: Veronderstel zonder verlies van algemeenheid dat de twee niet-nul symbolen 1 en -1 zijn en dat -1 het minste voorkomt. Het aantal keer dat -1 voorkomt noteren we als y. Neem een punt R met $c_R=1$ en een $(k-1)$-ruimte ρ die raakt aan $\mathcal{S}=\mathrm{supp}(c)$ in het punt R; dit kan door Stelling

3.1.4. Elke k-ruimte τ door ρ moet minstens nog één extra punt van $\mathcal{S}$ bevatten opdat $(c, \tau) = 0$. Er zijn zo θ_{n-k} verschillende k-ruimten en hoogstens y hiervan bevatten een punt met coördinaat -1. De overige $\theta_{n-k} - y$ verschillende k-ruimten door ρ moeten dan minstens $p-1$ extra punten met coördinaat 1 bevatten. Wanneer we dit aantal punten optellen, vinden we een ondergrens voor $w(c)$:

$$1 + y + (p-1)(\theta_{n-k} - y) \leq w(c).$$

Merk op dat deze ondergrens het kleinste is als y het grootste is, maar zelfs wanneer y maximaal is zullen we een strijdigheid vinden. In het geval dat $p = 7$, volgt er omdat -1 het minste vaak voorkomt dat $y \leq \frac{6\theta_{n-k}+1}{7}$ en dat $w(c) < \frac{12\theta_{n-k}+2}{7}$. Wanneer we dit substitueren, bekomen we volgende ongelijkheden:

$$\begin{aligned}
&1 + \frac{6\theta_{n-k}+1}{7} + (p-1)\left(\theta_{n-k} - \frac{6\theta_{n-k}+1}{7}\right) < \frac{12\theta_{n-k}+2}{7} \\
\iff &7 + 6\theta_{n-k} + 1 + (p-1)(7\theta_{n-k} - 6\theta_{n-k} - 1) < 12\theta_{n-k} + 2 \\
\iff &6 - 6\theta_{n-k} + (p-1)(\theta_{n-k} - 1) < 0 \\
\iff &7 - p + p\theta_{n-k} - 7\theta_{n-k} < 0.
\end{aligned}$$

Het linkerlid is echter nul als $p = 7$, wat een strijdigheid geeft. Als $p > 7$, dan is $w(c) < \frac{12\theta_{n-k}+6}{7}$ en $y \leq \frac{6\theta_{n-k}+3}{7}$. Dit geeft:

$$\begin{aligned}
&1 + \frac{6\theta_{n-k}+3}{7} + (p-1)\left(\theta_{n-k} - \frac{6\theta_{n-k}+3}{7}\right) < \frac{12\theta_{n-k}+6}{7} \\
\iff &7 + 6\theta_{n-k} + 3 + (p-1)(7\theta_{n-k} - 6\theta_{n-k} - 3) < 12\theta_{n-k} + 6 \\
\iff &4 - 6\theta_{n-k} + (p-1)(\theta_{n-k} - 3) < 0 \\
\iff &7 - 3p + (p-7)\theta_{n-k} < 0.
\end{aligned}$$

Dit geeft op zijn beurt een strijdigheid als $p > 7$. Men kan dit bijvoorbeeld inzien door te kijken naar het geval $p = 11$ en $k = n - 1$, wat het kleinste getal geeft. We hebben dus bewezen dat dit geval niet mogelijk is.

Geval 2: We gaan er nu van uit dat er vier verschillende niet-nul symbolen voorkomen in c, namelijk 1, -1, a en $-a$ met $a \in \mathbb{F}_p^*$. Het idee is hier dat we verschillende ondergrenzen zullen bepalen voor $w(c)$, die samen zullen leiden tot een strijdigheid. Beschouw een $(k-1)$-ruimte ρ die één punt van $\mathcal{S}$ bevat en zodat het aantal 2-secanten, zoals gedefinieerd in Lemma 3.3.1, door ρ minimaal is. We noemen het enige punt van $\mathcal{S}$ in ρ het punt R en het aantal 2-secanten door ρ noteren we hier als X_2. Merk op dat opnieuw elk symbool dan minstens X_2 keer voorkomt zoals gezien in Lemma 3.3.1. Aangezien we vier verschillende coëfficiënten hebben, weten we dan dat:

$$w(c) \geq 4X_2. \tag{3.1}$$

Wanneer een k-ruimte door ρ exact twee extra punten van $\mathcal{S}$ bevat, noemen we deze een 3-secant en dit aantal geven we weer met X_3. Alle andere k-ruimten door ρ snijden $\mathcal{S}$ in meer dan drie punten en dit aantal is X_w. Omdat er θ_{n-k} verschillende k-ruimten zijn door ρ, hebben we dat:

$$\theta_{n-k} = X_2 + X_3 + X_w. \tag{3.2}$$

Daarnaast kunnen we ook de punten tellen van $\mathcal{S}$ via de k-ruimten door ρ om een ondergrens te bepalen voor $w(c)$:

$$w(c) \geq 1 + X_2 + 2X_3 + 3X_w. \tag{3.3}$$

Veronderstel eerst dat er geen 3-secanten zijn, dan volgt uit (3.2) dat $X_2 = \theta_{n-k} - X_w$. Wanneer we dit substitueren in (3.1) en (3.3) vinden we dat:

$$\begin{cases} w(c) & \geq 4(\theta_{n-k} - X_w) \\ w(c) & \geq 1 + \theta_{n-k} + 2X_w \end{cases}$$

We tellen tweemaal de tweede vergelijking op bij de eerste om de term X_w te elimineren. De resulterende ongelijkheid is:

$$3w(c) \geq 2 + 6\theta_{n-k},$$

dit geeft echter een strijdigheid met de aanname dat $\frac{12\theta_{n-k}+6}{7} > w(c)$. Er bestaat dus altijd een 3-secant door ρ, stel dat τ zo een 3-secant is. We hebben dat $(c, \tau) = 0$, dus moet de som van de drie gebruikte symbolen in τ gelijk zijn aan $0 \pmod p$. Hierdoor is het niet toegelaten dat het codewoord c in τ zowel 1 als -1 gebruikt als coëfficiënt, want dan kan het niet dat $(c, \tau) = 0$. Analoog zien we in dat c in τ niet zowel a als $-a$ heeft als coëfficiënten. Veronderstel dat c in τ de symbolen 1 en a gebruikt. Het bewijs voor de koppels 1 en $-a$, -1 en a, en -1 en $-a$ is analoog. We gaan er ook vanuit dat voor het punt R in ρ geldt dat $c_R = 1$. Er zijn twee mogelijkheden ofwel bevat τ tweemaal 1 ofwel tweemaal a, in beide gevallen kunnen we bepalen wat a is:

$$\begin{aligned} 1 + 1 + a = 0 \pmod p \text{ en bijgevolg } a = -2, \\ 1 + a + a = 0 \pmod p \text{ en bijgevolg } a = -\frac{1}{2}. \end{aligned}$$

Voor een punt P met $c_P = -a$ geldt er dat de k-ruimte $\langle P, \rho \rangle = \sigma$ zeker nog een derde punt moet bevatten. Als σ exact drie punten van $\mathcal{S}$ bevat dan heeft het derde punt niet als coëfficiënt -1 of a omdat we al coëfficiënten 1 en a hebben. Er zijn dus maar twee mogelijkheden:

$$\begin{aligned} 1 + 1 - a = 0 \pmod p \text{ en } a = 2, \\ 1 - a - a = 0 \pmod p \text{ en } a = \frac{1}{2}. \end{aligned}$$

Maar de verzamelingen $\{-2, -1/2\}$ en $\{2, 1/2\}$ zijn disjunct omdat $p > 5$, wat een strijdigheid geeft. Dus bevat σ meer dan drie punten van $\mathcal{S}$. We weten ook dat er minstens X_2 punten zijn met coëfficiënt $-a$, die elk samen met ρ een deelruimte opspannen met meer dan drie punten van $\mathcal{S}$. Bijgevolg hebben we dat de k-ruimten met meer dan drie punten van $\mathcal{S}$ samen minstens X_2 extra punten van $\mathcal{S}$ bevatten. Door opnieuw de punten in k-ruimten door ρ te tellen en gebruik te maken van (3.2) vinden we nu volgende ondergrens voor $w(c)$:

$$\begin{aligned} w(c) &\geq 1 + X_2 + 2X_3 + 3X_w \\ &\geq 1 + X_2 + 2X_3 + X_2 \\ &= 1 + 2(\theta_{n-k} - X_3 - X_w) + 2X_3 \\ &= 1 + 2\theta_{n-k} - 2X_w. \end{aligned}$$

We kunnen ook (3.2) substituren in (3.1) en (3.3) om twee andere ondergrenzen te vinden voor $w(c)$:

$$\begin{cases} w(c) & \geq 4(\theta_{n-k} - X_3 - X_w) \\ w(c) & \geq 1 + \theta_{n-k} + X_3 + 2X_w. \end{cases}$$

Wanneer we nu twee keer de eerste ondergrens met één keer de tweede ondergrens en vier keer de derde ondergrens optellen, elimineren we de termen in X_3 en X_w. De ongelijkheid wordt:

$$7w(c) \geq 6 + 12\theta_{n-k}.$$

Dit is overduidelijk in strijd met onze assumptie dat $w(c) < \frac{6+12\theta_{n-k}}{7}$, waarmee we ook dit geval hebben bewezen. ∎

Dezelfde auteurs hebben in het eerdere artikel [25] een andere grens bewezen die enkel geldt voor hypervlakken. Namelijk door op zeer gelijkaardige manier als hierboven een grens te bepalen voor het minimum gewicht van $\mathcal{C}_1(2,q)^\perp$. Vervolgens kan men dit uitbreiden via de gelijkheid in Stelling 3.3.8 die we later zullen bewijzen. De gelijkheid uit Stelling 3.3.8 zal de basis vormen voor het tweede type ondergrens dat we in het volgende deel bewijzen. De stelling voor hypervlakken geven we hier zonder bewijs. De algemenere grens, hier Stelling 3.3.3, die ze later bewezen is immers beter voor $p = 7$ en hetzelfde voor $p \geq 7$.

Stelling 3.3.4. *[25, Theorem 18] Als $p = 7$, dan is het minimum gewicht van $\mathcal{C}_{n-1}(n,q)^\perp$ minstens $\frac{12q+7}{7}$. Als $p > 7$, dan is het minimum gewicht minstens $\frac{12q+18}{7}$.*

3.3.2. Ondergrens via projecteren

We kunnen een codewoord van $C_k(n,q)^\perp$ omzetten naar een codewoord van $C_{k-1}(n-1,q)^\perp$. Dit zullen we gebruiken om aan te tonen dat deze twee codes hetzelfde minimum gewicht hebben. Deze redenering is gebaseerd op [26] van Lavrauw, Storme en Van de Voorde. We bespreken eerst hoe dit omzetten juist gebeurt.

Definitie 3.3.5 (Projectie van een codewoord c). Gegeven zijn een codewoord $c \in \mathcal{C}_k(n,q)^\perp$, een punt R en een hypervlak π waar R niet in ligt. We definiëren voor elk punt $P \in \pi$ het getal c'_P als $\sum c_{P_i}$, met c_{P_i} de coördinaten van de punten P_i uit de verzameling $\mathcal{S} \cap \langle R, P\rangle$, met $\mathcal{S} = \text{supp}(c)$. De vector c' die bestaat uit de coördinaten c'_P, $P \in \pi$, noemen we dan de projectie van c uit R op π.

Lemma 3.3.6. *De projectie c' van een codewoord $c \in \mathcal{C}_k(n,q)^\perp$ uit R op een hypervlak π met $R \notin \pi$ is een codewoord van $C_{k-1}(n-1,q)^\perp$.*

Bewijs. Veronderstel dat het c' de projectie is van een codewoord $c \in \mathcal{C}_k(n,q)^\perp$ uit een punt R op een hypervlak π met $R \notin \pi$. Neem vervolgens een willekeurige $(k-1)$-ruimte ρ' in π. We breiden deze uit naar de k-ruimte $\rho = \langle \rho', R\rangle$. Er geldt dat $0 = (c, \rho)$, merk op dat dit wil zeggen dat de som van de coördinaten van c over de punten uit ρ gelijk is aan 0. Nu is deze som per constructie gelijk aan de som van de coördinaten van c' over de punten van ρ'. Merk op dat als $R \in \text{supp}(c)$, de coördinaat c_R juist $1 \pmod p$ keer voorkomt, dus ook dan zijn deze sommen gelijk. Hierdoor vinden we dat $(c', \rho') = 0$. Aangezien ρ' willekeurig gekozen is en de $(k-1)$-deelruimten de code $\mathcal{C}_{k-1}(n-1,q)$ voortbrengen, hebben we bewezen dat c' inderdaad een codewoord is van $\mathcal{C}_{k-1}(n-1,q)^\perp$. ∎

Nu we weten dat projecteren opnieuw een codewoord geeft, kunnen we aantonen dat hierdoor het minimum gewicht van $C_k(n,q)^\perp$ en $C_{k-1}(n-1,q)^\perp$ en bij uitbreiding $d(\mathcal{C}_1(n-k+1,q)^\perp)$ hetzelfde is.

Lemma 3.3.7. *[26, Lemma 11] Volgende ongelijkheid geldt voor alle $n \geq 2$ en $0 < k \leq n-1$:*

$$d(\mathcal{C}_k(n,q)^\perp) \geq d(\mathcal{C}_{k-1}(n-1,q)^\perp) \geq \cdots \geq d(\mathcal{C}_1(n-k+1,q)^\perp).$$

Bewijs. Beschouw een codewoord $c \in \mathcal{C}_k(n,q)^\perp$ met minimum gewicht en een punt $R \notin \mathcal{S} = \mathrm{supp}(c)$. Neem ook een hypervlak π dat R niet bevat en noem c' de projectie van c uit R op π. Het is duidelijk dat $|\mathrm{supp}(c')| \leq |\mathrm{supp}(c)|$ en dus vinden we dat $w(c') \leq w(c)$. Omdat c een codewoord van minimum gewicht is besluiten we dat $d(\mathcal{C}_k(n,q)^\perp) \geq d(\mathcal{C}_{k-1}(n-1,q)^\perp)$. Deze redenering geldt voor alle n en k, zodoende hebben we de stelling bewezen. ■

We tonen vervolgens aan dat dat deze ongelijkheid een gelijkheid is.

Stelling 3.3.8. *[26, Theorem 10] Voor alle $n \geq 2$ en $0 < k \leq n-1$ geldt er dat:*

$$d(\mathcal{C}_k(n,q)^\perp) = d(\mathcal{C}_{k-1}(n-1,q)^\perp) = \cdots = d(\mathcal{C}_1(n-k+1,q)^\perp).$$

Bewijs. We beginnen met $\pi = \mathrm{PG}(n-k+1,q)$ te embedden in $\mathrm{PG}(n,q)$ en elk codewoord c van $\mathcal{C}_1(\pi)^\perp$ uit te breiden naar een vector c^n van $V(\theta_n,p)$ door een nul te plaatsen voor alle punten $P \in \mathrm{PG}(n,q) \setminus \pi$. In de code $\mathcal{C}_1(\pi)$ is de vector v bestaande uit allemaal énen een codewoord. We kunnen dit codewoord maken door alle codewoorden uit de incidentiematrix G op te tellen, immers ligt elk punt op $\theta_{n-k} = 1 \pmod p$ rechten in $\mathrm{PG}(n-k+1,q)$. Hieruit volgt er dat $\sum_{P\in\pi} c^n_P = (c,v) = 0$ voor elke $c \in \mathcal{C}_1(\pi)^\perp$. Daardoor vinden we voor elke k-ruimte σ in $\mathrm{PG}(n,q)$ die π bevat dat $(c^n,\sigma) = 0$. Een k-ruimte σ in $\mathrm{PG}(n,q)$ die π niet bevat, snijdt π minstens in een rechte door de grootte van de dimensies. We kunnen $\sigma \cap \pi$ dan ook beschrijven als een bundel $\mathcal{A}$ van rechten l door een zeker punt P. Dit aantal rechten is $1 \pmod p$. Daarnaast weten we dat voor elke rechte l geldt dat $(c,l) = 0$ omdat per definitie $l \subseteq \pi$, dus hebben we dat:

$$(c^n, \sigma \cap \pi) = \left(c^n, \sum_{l\in\mathcal{A}} l\right) = \sum_{l\in\mathcal{A}} (c^n, l) = 0.$$

Aangezien c^n nul is voor de punten buiten π, volgt hieruit onmiddellijk dat $(c^n,\sigma) = 0$ en dus $c^n \in \mathcal{C}_k(n,q)^\perp$. Daarnaast is het gewicht van c^n gelijk aan het gewicht van c en kunnen we dus constateren dat $d(\mathcal{C}_k(n,q)^\perp) \leq d(\mathcal{C}_1(n-k+1,q)^\perp)$. De ongelijkheid uit de vorige stelling wordt hiermee een gelijkheid en dit is wat we wilden bewijzen. ■

We bepalen vervolgens een ondergrens voor het minimum gewicht van de code $\mathcal{C}_1(n,q)^\perp$. Deze kunnen we dan via de vorige stelling uitbreiden naar andere codes. We geven hier het korte bewijs van Adriaensen uit [1]. Het originele bewijs van de stelling, [8, Theorem 2] door Bagchi en Inamdar, volgt een andere aanpak en toont ook bijkomende eigenschappen aan in geval van gelijkheid.

Stelling 3.3.9. *[1, Result 3.2] Beschouw positieve getallen λ en n. Gegeven een incidentiestructuur $(\mathcal{P},\mathcal{B})$, waarbij elk punt bevat is in minstens $n+\lambda$ blokken en elk paar punten in hoogstens λ blokken ligt. Voor een niet-nul codewoord $c \in \mathcal{C}^\perp$, met $\mathcal{C}$ de code gevormd door de incidentiestructuur over het priemveld $\mathbb{F}_p$, geldt er dat:*

$$w(c) \geq 2\left(\frac{n+\lambda}{\lambda} - \frac{n}{\lambda p}\right).$$

Bewijs. Voor elk niet-nul codewoord $c \in \mathcal{C}^\perp$ kunnen we een multi verzameling $\mathcal{M}(c)$ definiëren bestaande uit de punten van $\mathrm{supp}(c) = \mathcal{S}$. Elk punt P heeft in deze verzameling een multipliciteit die gelijk is aan zijn coëfficiënt c_P in c. Veronderstel nu dat $c \in \mathcal{C}^\perp$ een codewoord is met minimum gewicht. Aangezien er zeker een punt P bestaat zodat $c_P \neq 0$, kunnen we c herschalen zodat $c_P = 1$. We bepalen eerst een ondergrens voor de grootte van $\mathcal{M}(c)$. We weten dankzij het gegeven dat er minstens $n+\lambda$ blokken zijn door P. Elk zo'n blok correspondeert met een codewoord $c' \in \mathcal{C}$, waarvoor moet gelden dat $(c,c') = 0 \pmod p$. Dus geldt er dat c nog minstens $p-1$ andere punten moet bevatten van elk blok, let op dat we hierbij tellen volgens multipliciteit. Elk extra punt Q dat

we vinden, kunnen we maximaal in λ blokken opnieuw tellen. Immers ligt P ook in elk blok en door het gegeven liggen P en Q samen hoogstens in λ blokken. Dus volgt er dat:

$$|\mathcal{M}(c)| \geq 1 + \frac{n+\lambda}{\lambda}(p-1) = \frac{n+\lambda}{\lambda}p - \frac{n}{\lambda}.$$

We onderscheiden nu twee gevallen. Stel eerst dat er geen enkel punt $R \in \mathcal{P}$ is zodat $c_R = -1$. Dan moet elk blok door P minstens twee extra punten bevatten, opdat er voor de corresponderende codewoorden geldt: $(c, c') = 0$. Hieruit volgt dat $w(c) \geq 1 + 2\frac{n+\lambda}{\lambda}$, wat sterker is dan het te bewijzen. Veronderstel nu dat er wel een punt $R \in \mathcal{P}$ bestaat met $c_R = -1$. Dan geldt er voor het codewoord $-c$ dat $(-c)_R = 1$ en kunnen we bovenstaande redenering herhalen zodat:

$$|\mathcal{M}(-c)| \geq \frac{n+\lambda}{\lambda}p - \frac{n}{\lambda}.$$

Voor elk punt $S \in \mathcal{S}$ geldt er dat als het multipliciteit $\alpha = c_S$ heeft in $\mathcal{M}(c)$, dan heeft het multipliciteit $p - \alpha = (-c)_S$ in $\mathcal{M}(-c)$. Dus volgt er dat

$$|\mathcal{M}(c)| + |\mathcal{M}(-c)| = \sum_{S \in \mathcal{S}} c_S + (-c)_S = \sum_{S \in \mathcal{P}} (\alpha + p - \alpha) = pw(c).$$

Hieruit kunnen we dan besluiten dat ook in dit geval geldt:

$$w(c) = \frac{|\mathcal{M}(c)| + |\mathcal{M}(-c)|}{p} \geq \frac{2}{p}\left(\frac{n+\lambda}{\lambda}p - \frac{n}{\lambda}\right).$$

■

Deze algemene stelling over de ondergrens voor het minimum gewicht van de duale code van een code geïnduceerd door een incidentiestructuur, kunnen we toepassen op $\mathcal{C}_1(n,q)^\perp$. Dit geeft de volgende ondergrens:

Stelling 3.3.10. *[1, Corollary 3.3] Er geldt voor $q = p^h$, met p priem, dat*

$$d(\mathcal{C}_1(n,q)^\perp) \geq 2\left(\theta_{n-1}\left(1 - \frac{1}{p}\right) + \frac{1}{p}\right).$$

Bewijs. Dit volgt rechtstreeks uit de vorige stelling: we weten dat elk paar punten bevat is in juist één rechte, dus $\lambda = 1$. Elk punt is bevat in θ_{n-1} rechten, dus kiezen we $n = \theta_{n-1} - 1$. Hieruit volgt dat voor een niet-nul codewoord $c \in \mathcal{C}_1(n,q)^\perp$ geldt:

$$w(c) \geq 2\left(\frac{n+\lambda}{\lambda} - \frac{n}{\lambda p}\right) = 2\left(1 + \theta_{n-1} - 1 - \frac{\theta_{n-1} - 1}{p}\right) = 2\left(\theta_{n-1}\left(1 - \frac{1}{p}\right) + \frac{1}{p}\right).$$

Dit bewijst het gevraagde. ■

Wanneer we de gevonden stellingen combineren, vinden we de beloofde tweede ondergrens:

Gevolg 3.3.11. *Er geldt voor $q = p^h$, met p priem, dat*

$$d(\mathcal{C}_k(n,q)^\perp) \geq 2\left(\theta_{n-k}\left(1 - \frac{1}{p}\right) + \frac{1}{p}\right).$$

Bewijs. Dit volgt rechtstreeks uit de bovenstaande stellingen en Stelling 3.3.8. ■

Het is ook mogelijk om Stelling 3.3.9 rechtstreeks toe te passen op $\mathcal{C}_k(n,q)^\perp$.

Stelling 3.3.12. *[8, Theorem 3] Er geldt voor $q = p^h$, met p priem, dat*

$$d(\mathcal{C}_k(n,q)^\perp) \geq 2\left(\frac{q^n-1}{q^k-1}\left(1-\frac{1}{p}\right)+\frac{1}{p}\right).$$

Bewijs. Dit is analoog aan het bewijs voor $d(\mathcal{C}_1(n,q)^\perp)$. ∎

Dit blijkt echter een minder goede grens te zijn, omdat:

$$\begin{aligned}\theta_{n-k} = \frac{q^{n-k+1}-1}{q-1} \geq \frac{q^n-1}{q^k-1} &\iff q^{n+1}-q^k-q^{n-k+1}+1 \geq q^{n+1}-q-q^n+1\\ &\iff q^{n-1}+1 \geq q^{n-k}+q^{k-1}\end{aligned}$$

Als $k=1$, dan zijn de twee ondergrenzen duidelijk even goed. Maar wanneer $k>1$, dan is dit een strikte ongelijkheid en bijgevolg geeft Stelling 3.3.11 het beste resultaat.

3.3.3. Ondergrens via affiene ruimten

In deze subsectie tonen we een derde en laatste ondergrens aan voor het minimum gewicht van $\mathcal{C}_k(n,q)^\perp$. Later bewijzen we dat deze ondergrens wordt bereikt als q even is. Om de derde grens te bewijzen, hebben we een ondergrens nodig voor het minimum gewicht van de code $\mathcal{C}_k(\mathrm{AG}(n,q))^\perp$. De code $\mathcal{C}_k(\mathrm{AG}(n,q))$ is analoog aan $\mathcal{C}_k(n,q)$ gedefinieerd via de incidentiematrix van punten en k-ruimten in $\mathrm{AG}(n,q)$. De duale code noteren we als $\mathcal{C}_k(\mathrm{AG}(n,q))^\perp$. We nemen volgend resultaat voor het minimum gewicht van de code $\mathcal{C}_k(\mathrm{AG}(n,q))^\perp$ aan zonder bewijs.

Stelling 3.3.13. *[7, Theorem 5.7.9] Het minimum gewicht van $\mathcal{C}_k(\mathrm{AG}(n,q))^\perp$, met $q=p^h$, is minstens $(q+p)q^{n-k-1}$.*

We bewijzen nu de beloofde derde ondergrens voor het minimum gewicht van $\mathcal{C}_k(n,q)^\perp$ zoals Calkin, Key en Resmini.

Stelling 3.3.14. *[13, Proposition 1] Het minimum gewicht van $\mathcal{C}_k(n,q)^\perp$, met $q=p^h$, is minstens $(q+p)q^{n-k-1}$.*

Bewijs. Neem een codewoord $c \in \mathcal{C}_k(n,q)^\perp$ en noteer de bijhorende support als $\mathcal{S}$. We splitsen het bewijs op in twee gevallen. Veronderstel eerst dat er een hypervlak π bestaat zodat $\mathcal{S}\cap\pi = \emptyset$. Door dit hypervlak weg te laten, zien we dat c ook een codewoord is van $\mathcal{C}_k(\mathrm{AG}(n,q))^\perp$. Uit Stelling 3.3.13 volgt dat $w(c) \geq (q+p)q^{n-k-1}$. Vanaf nu kunnen we er dus vanuit gaan dat elk hypervlak minstens één punt gemeen heeft met $\mathcal{S}$. We bewijzen de stelling via inductie op n. We definiëren de verzameling $\{n_1,\ldots,n_r\}$ als de verzameling van alle intersectie groottes die voorkomen tussen een hypervlak en $\mathcal{S}$. We nemen zonder verlies van algemeenheid aan dat $n_1 < n_2 < \cdots < n_r$ en dat er x_{n_i} hypervlakken zijn die exact n_i punten gemeen hebben met $\mathcal{S}$, met $i \in \{1,\ldots,r\}$. We kunnen het aantal hypervlakken in $\mathrm{PG}(n,q)$ tellen door al deze x_{n_i} te sommeren. Aangezien er θ_n verschillende hypervlakken zijn, geeft dit:

$$x_{n_1}+\cdots+x_{n_r} = \frac{q^{n+1}-1}{q-1}.$$

Vervolgens tellen we het aantal koppels (P,π), met P een punt en π een hypervlak zodat $P \in \mathcal{S}\cap\pi$, op twee manieren. De eerste manier gebruikt dat er x_{n_i} hypervlakken zijn die exact n_i punten van $\mathcal{S}$ bevatten. Wanneer we dan de termen $n_i x_{n_i}$ optellen voor alle $i \in \{1,\ldots,r\}$ vinden we het

gezochte aantal koppels. De tweede manier is gebaseerd op het feit dat er door elk punt van $\mathcal{S}$ juist θ_{n-1} hypervlakken gaan. Dit resulteert in de volgende gelijkheid:

$$n_1 x_{n_1} + \cdots + n_r x_{n_r} = |\mathcal{S}| \frac{q^n - 1}{q - 1}.$$

Vermenigvuldigen we vervolgens de eerste vergelijking met n_1 dan is het linkerlid van deze nieuwe vergelijking kleiner dan het linkerlid van de tweede vergelijking omdat $n_1 < n_2 < \cdots < n_r$. We bekomen uit de rechterleden van deze vergelijkingen dan dat:

$$|\mathcal{S}| \frac{q^n - 1}{q - 1} \geq n_1 \frac{q^{n+1} - 1}{q - 1} \iff |\mathcal{S}| \geq n_1 \frac{q^{n+1} - 1}{q^n - 1} \geq n_1 q.$$

Via de gevonden vergelijkingen kunnen we nu de inductiebasis, $n = 2$ en $k = 1$, aantonen. Elk hypervlak, hier dus elke rechte, heeft een punt gemeen met $\mathcal{S}$ per aanname. Aangezien $k = 1$, moet elke rechte l dan minstens nog één ander punt bevatten van $\mathcal{S}$ opdat $(c, l) = 0$. Hieruit vinden we dat $n_1 \geq 2$. Als we dit invullen in bovenstaande ongelijkheid geeft dat $|\mathcal{S}| \geq 2q \geq q + p$, wat we moesten bewijzen. We nemen vanaf nu aan dat de inductiehypothese, het minimum gewicht van $\mathcal{C}_k(m, q)^\perp$ is gelijk aan $(q + p)q^{m-k-1}$ voor alle $m < n$ en $1 \leq k \leq m - 1$, waar is. Stel dat $\mathcal{S}$ de support is van een codewoord $c \in \mathcal{C}_k(n, q)^\perp$. We veronderstellen ook nog steeds dat elk hypervlak minstens één punt gemeen heeft met $\mathcal{S}$. In het geval $k = n - 1$, vinden we opnieuw dat $n_1 \geq 2$ en geeft dit $|\mathcal{S}| \geq 2q \geq q + p$. We zijn dus meteen klaar met dit geval. Stel nu dat $k < n - 1$, dan kunnen we de inductiehypothese toepassen door $\mathcal{S}$ te beperken tot een hypervlak. Aangezien n_1 het minimum aantal punten is van $\mathcal{S}$ in een hypervlak vinden we $n_1 \geq (q + p)q^{(n-1)-k-1}$. Wanneer we dit substitueren in bovenstaande ongelijkheid bekomen we

$$|\mathcal{S}| \geq (q + p)q^{(n-1)-k-1} q = (q + p)q^{n-k-1}.$$

Hiermee hebben we bewezen wat we wilden bewijzen. ■

3.3.4. Minimum gewicht als $q = p$, met p priem

Zoals eerder gezegd kunnen we voor $q = p$, met p priem, het minimum gewicht van $\mathcal{C}_k(n, q)^\perp$ exact bepalen. Dat is het doel van dit deel. Hiervoor hebben we enkele andere stellingen nodig uit [26] van Lavrauw, Storme en Van de Voorde, die we eerst bewijzen.

Lemma 3.3.15. *[26, Lemma 12] Zij $\mathcal{A}$ een puntenverzameling in $\mathrm{PG}(n, q)$ zodat er voor elk punt $P \in \mathrm{PG}(n, q) \setminus \mathcal{A}$, dat ligt op een secant rechte aan $\mathcal{A}$, geldt dat P op geen enkele raaklijn aan $\mathcal{A}$ ligt. Als ook $\dim(\langle \mathcal{A} \rangle) \geq n - k + 2$, dan is $|\mathcal{A}| \geq \theta_{n-k+1}$.*

Bewijs. We tonen eerst via inductie aan dat er een punt $P \in \mathcal{A}$ en een r-ruimte ρ, met $2 \leq r \leq n - k + 2$, bestaan zodat alle rechten door P in de deelruimte ρ secanten zijn aan $\mathcal{A}$. We bedoelen met het begrip secant hier een rechte die minstens twee punten van $\mathcal{A}$ bevat. Hiermee zullen we nadien het te bewijzen aantonen. Voor de inductiebasis bekijken we een vlak π opgespannen door drie punten P, Q en R van $\mathcal{A}$. Neem een willekeurige rechte l door P in π. Als de rechte l de rechte $m = \langle Q, R \rangle$ snijdt in een punt van $\mathcal{A}$ zoals Q of R dan is l een secant. Wanneer l de rechte m snijdt in een punt $S \notin \mathcal{A}$, dan is l ook een secant. Want stel dat l een raaklijn is, dan ligt het punt S op de raaklijn l en de secant m, wat niet kan door het gegeven. We hebben de inductiebasis dus bewezen. Veronderstel nu dat er een r-ruimte τ bestaat zodat alle rechten door P secanten zijn, met $2 \leq r < n - k + 2$. Er bestaat steeds een punt $T \in \mathcal{A}$ zodat $T \notin \tau$ omdat $\dim(\langle \mathcal{A} \rangle) \geq n - k + 2$. De rechte $\langle P, T \rangle$ is duidelijk een secant. Neem willekeurig een andere rechte l door P in $\langle \tau, T \rangle$. We

tonen aan dat l ook een secant is. Het vlak $\langle l, T\rangle \subseteq \langle \tau, T\rangle$ snijdt τ in een rechte m door het punt P. Door de inductiehypothese is m een secant aan $\mathcal{A}$ en omdat $T \notin m$ is $\langle m, T\rangle$ een vlak opgespannen door punten van $\mathcal{A}$. Aangezien $l \subset \langle m, T\rangle$ volgt er zoals in het bewijs voor de inductiebasis dat l een secant is. Bijgevolg bestaat er een $(r+1)$-ruimte ρ, namelijk $\langle \tau, T\rangle$, zodat elke rechte door P een secant is. Als we $r = n-k+1$ kiezen, dan zijn er door P juist θ_{n-k+1} rechten in ρ die elk nog minstens één extra punt van $\mathcal{A}$ bevatten. Dit toont aan dat $|\mathcal{A}| \geq \theta_{n-k+1}$, wat we wilden bewijzen. ■

Stelling 3.3.16. *[26, Theorem 11] Een codewoord $c \in \mathcal{C}_k(n,q)^\perp$ met minimum gewicht is bevat in een $(n-k+1)$-ruimte van $\mathrm{PG}(n,q)$.*

Bewijs. Neem $c \in \mathcal{C}_k(n,q)^\perp$ zodat c een codewoord is met minimum gewicht. We noteren $\mathrm{supp}(c)$ als $\mathcal{S}$. Zoals eerder gezien is $w(c) \leq 2q^{n-k}$. Veronderstel dat $\dim(\langle \mathcal{S}\rangle) \geq n-k+2$. Omdat $w(c) \leq 2q^{n-k}$ is de conclusie van Lemma 3.3.15 niet waar voor de verzameling $\mathcal{S}$. Uit de negatie van dit lemma volgt dat er een punt $R \in \mathrm{PG}(n,q) \setminus \mathcal{S}$ bestaat waardoor er minstens één raaklijn en minstens één secant aan $\mathcal{S}$ gaan. We projecteren het codewoord c precies $k-1$ keer vanuit het punt R zodat we een codewoord $c' \in \mathcal{C}_1(n-k+1,q)^\perp$ krijgen. We noemen de $(n-k+1)$-ruimte waar $\mathrm{supp}(c')$ in bevat is ρ. Aangezien er door R minstens één secant aan $\mathcal{S}$ is, volgt er dat we bij het projecteren zeker één punt van $\mathcal{S}$ "verliezen". Bijgevolg is $0 < w(c') < w(c)$, en uit Stelling 3.3.8 halen we dat $0 < w(c') \leq w(c) - 1 < d(\mathcal{C}_1(n-k+1,q)^\perp)$. Dit geeft een strijdigheid en dus is $\dim(\langle \mathcal{S}\rangle) < n-k+2$. ■

We bepalen vervolgens het minimum gewicht van $\mathcal{C}_1(n,p)^\perp$ zoals Bagchi en Inamdar. Nadien zullen we dit uitbreiden naar willekeurige k op dezelfde manier als Lavrauw, Storme en Van de Voorde.

Stelling 3.3.17. *[8, Proposition 2] Het minimum gewicht van de code $\mathcal{C}_1(n,p)^\perp$ is $2p^{n-1}$. De codewoorden van minimum gewicht zijn de scalaire veelvouden van het verschil van twee verschillende hypervlakken.*

Bewijs. Als we in de ondergrens voor het minimum gewicht uit Stelling 3.3.11 gebruiken dat $q = p$, vinden we als ondergrens:

$$2\left(\theta_{n-1}\left(1-\frac{1}{p}\right)+\frac{1}{p}\right) = 2\left(\theta_{n-1}-\theta_{n-2}-\frac{1}{p}+\frac{1}{p}\right) = 2p^{n-1}.$$

We weten ook dat het verschil van twee hypervlakken een codewoord is met dit gewicht. Dus hebben we bewezen dat $2p^{n-1}$ het minimum gewicht is van de code $\mathcal{C}_1(n,p)^\perp$. We bewijzen hier niet dat dit de enige codewoorden zijn met dit gewicht. De geïnteresseerde lezer kan het bewijs in [8, Proposition 2] nalezen. Daar wordt een meer algemene versie van deze stelling bewezen, want ze bepalen het minimum gewicht en karakteriseren codewoorden met dit gewicht van de code $\mathcal{C}_{k-1,k}(n,p)^\perp$. Het bewijs steunt onder andere op hun bewijs van Stelling 3.3.9 waaruit ze zoals eerder vermeld meer eigenschappen kunnen afleiden in geval van gelijkheid. ■

Stelling 3.3.18. *[26, Theorem 12] Het minimum gewicht van $\mathcal{C}_k(n,p)^\perp$ is $2p^{n-k}$. De codewoorden met dit gewicht zijn de scalaire veelvouden van het verschil van twee verschillende $(n-k)$-ruimten die snijden in een $(n-k-1)$-ruimte.*

Bewijs. Stel dat $c \in \mathcal{C}_k(n,p)^\perp$ een codewoord is met minimum gewicht. Uit Stelling 3.3.16 weten we dat er een $(n-k+1)$-ruimte ρ bestaat zodat $\mathrm{supp}(c) \subseteq \rho$. We projecteren $k-2$ keer zodat we dan kunnen projecteren naar ρ. Al deze $k-1$ projecties laten c onveranderd, want $\mathrm{supp}(c) \subseteq \rho$. Dus is $c \in \mathcal{C}_1(n-k+1,p)^\perp$. Uit Stelling 3.3.17 weten we dat c in ρ een scalair veelvoud is van het verschil van twee verschillende hypervlakken. In $\mathrm{PG}(n,p)$ betekent dit dat c een scalair veelvoud

is van het verschil van twee verschillende $(n-k)$-ruimten die snijden in een $(n-k-1)$-ruimte. Hieruit volgt dat $w(c) = 2p^{n-k}$. Merk op dat we evengoed zoals in het bewijs van de vorige stelling via Stelling 3.3.11 hadden kunnen bepalen wat het minimum gewicht is. ■

Hiermee hebben we dus gevonden dat het minimum gewicht van $\mathcal{C}_k(n,p)^\perp$ gelijk is aan $2p^{n-k}$. Ook weten we nu dat deze codewoorden het scalair veelvoud zijn van het verschil van twee $(n-k)$-ruimten die snijden in een $(n-k-1)$-ruimte. Daardoor zouden we kunnen vermoeden dat ook voor andere q geldt dat het minimum gewicht gelijk is aan $2q^{n-k}$ en dat deze codewoorden van dezelfde vorm zijn. We hebben immers nog geen voorbeelden gezien van kleinere codewoorden. Dit vermoeden blijkt echter niet waar te zijn. Voor q even kunnen we ook aantonen wat het minimum gewicht is en dit toont aan dat deze hypothese vals is.

3.3.5. Minimum gewicht als q even is

Zoals hierboven besproken kunnen we ook voor q even aantonen wat het minimum gewicht is. Dankzij Stelling 3.3.8 weten we dat het voldoende is om dit te bewijzen voor $k = 1$. Wanneer $q = 2^h$, is een codewoord van $\mathcal{C}_1(n,q)^\perp$ hetzelfde als een even verzameling. Inderdaad, als $c \in \mathcal{C}_1(n,q)^\perp$, dan heeft $\mathrm{supp}(c)$ een even aantal punten gemeen met elke rechte l in $\mathrm{PG}(n,q)$ opdat $(c,l) = 0$. Dus is $\mathrm{supp}(c)$ een even verzameling. Ook is het duidelijk dat elke even verzameling een support vormt voor een codewoord van $\mathcal{C}_1(n,q)^\perp$. We mogen dus inderdaad zeggen dat de codewoorden van $\mathcal{C}_1(n,q)^\perp$, met q even, corresponderen met even verzamelingen. Ons doel is om aan te tonen dat voor $q = 2^h$ de ondergrens voor het minimum gewicht uit Stelling 3.3.14 wordt bereikt. We baseren ons hiervoor op [13] van Calkin, Key en Resmini. We bespreken eerst hoe we even verzamelingen in een projectieve ruimte kunnen uitbreiden naar even verzamelingen in projectieve ruimten met hogere dimensies. Nadien bewijzen we onmiddellijk via een constructie die gebaseerd is op dit principe, dat de ondergrens uit 3.3.14 bereikt wordt.

Stelling 3.3.19. *[13, Proposition 2] Gegeven een verzameling $\mathcal{S}$ bestaande uit punten die bevat zijn in een hypervlak π van $\mathrm{PG}(n,q)$ zodat $\mathcal{S}$ in dit hypervlak een even verzameling vormt. Beschouw een punt $P \notin \pi$. De verzameling*

$$\mathcal{S}' = \{Q |\ \textit{het punt } Q \textit{ ligt op een rechte } \langle P,R\rangle \textit{ met } R \in \mathcal{S}\} \setminus \{P\}$$

is een even verzameling in $\mathrm{PG}(n,q)$, $q = 2^h$, met grootte $q|\mathcal{S}|$.

Bewijs. We controleren voor elke rechte l of deze een even aantal punten bevat van $\mathcal{S}'$. Als $l \subseteq \pi$, dan is dit waar omdat in dit geval $l \cap \mathcal{S} = l \cap \mathcal{S}'$ en $\mathcal{S}$ een even verzameling vormt in π. Als $l \nsubseteq \pi$, dan is $l \cap \pi$ een punt R. We bespreken eerst het geval waarin $R \in \mathcal{S}$. Als $l = \langle R,P\rangle$, dan bevat l per constructie q punten van $\mathcal{S}'$. Omdat q even is, is dit deelgeval voldaan. In het andere deelgeval, $P \notin l$, bekijken we het vlak τ door l en P. Dit vlak snijdt π noodzakelijk in een rechte m. Aangezien $R \in \mathcal{S} \cap m$, bevat m nog een oneven aantal andere punten van $\mathcal{S}$. Elk zo'n punt ligt op een rechte e met P in het vlak τ. Alle punten op de rechte e behalve het punt P, behoren tot $\mathcal{S}'$ bij constructie. Bijgevolg snijdt l elke rechte e in een verschillend punt van $\mathcal{S}'$ en samen met R vinden we dus een even aantal punten in $l \cap \mathcal{S}'$.

Het tweede geval dat we moeten bespreken is $R \notin \mathcal{S}$. We bekijken opnieuw eerst het deelgeval waarin $l = \langle R,P\rangle$. Het is duidelijk dat l door de definitie van $\mathcal{S}'$ geen enkel punt van $\mathcal{S}'$ bevat, wat dit geval afrondt. Als $P \notin l$, kunnen we opnieuw het vlak τ door het punt P en de rechte l bekijken en hieruit de rechte $m = \tau \cap \pi$ definiëren. Het even aantal punten van $m \cap \mathcal{S}$ bepaalt het even aantal punten van $l \cap \mathcal{S}'$ via de rechten door een punt van $m \cap \mathcal{S}$ en P zoals voordien. Merk

op dat het nu wel kan dat m geen enkel punt van $\mathcal{S}$ bevat. Dan is ook $l \cap \mathcal{S}' = \emptyset$. Daarmee is dit bewijs afgerond. ■

Stelling 3.3.20. *[13, Theorem 1] Het minimum gewicht van de code $\mathcal{C}_k(n,q)^\perp$, met $q = 2^h$, is $q^{n-k-1}(q+2)$.*

Bewijs. We bewijzen de stelling eerst voor het geval $k = 1$ zoals gedaan in [13, Corollary 1]. We weten al dat het minimum gewicht minstens $q^{n-2}(q+2)$ is dankzij Stelling 3.3.14. Wanneer we zoals eerder gezegd een voorbeeld geven van een codewoord met dit gewicht, is dit geval bewezen. Neem een vlak π in $\mathrm{PG}(n,q)$ en beschouw een reguliere hyperovaal in π. Deze hyperovaal is een even verzameling met grootte $q+2$. Vervolgens beschouwen we een 3-ruimte door π. We breiden onze even verzameling uit zoals beschreven in de vorige stelling. Bijgevolg hebben we al een even verzameling in $\mathrm{PG}(3,q)$ gevonden met grootte $(q+2)q$. We kunnen deze opnieuw uitbreiden via de vorige stelling en de redenering inductief herhalen tot we een even verzameling van grootte $(q+2)q^{n-2}$ vinden in $\mathrm{PG}(n,q)$. Zo hebben we het geval $k = 1$ bewezen. Als $k > 1$, dan weten we dat $d(\mathcal{C}_k(n,q)^\perp) = d(\mathcal{C}_1(n-k+1,q)^\perp) = (q+2)q^{n-k-1}$ dankzij Stelling 3.3.8. Merk op dat deze laatste stap in [13] op een iets andere manier wordt bewezen. Wij kunnen echter onmiddellijk Stelling 3.3.8 toepassen en op deze manier het bewijs wat inkorten. Wanneer de geïnteresseerde lezer dit bewijs zou nalezen, is het aangeraden om eerst de algemenere definitie voor even verzamelingen aan de hand van designs die men daar hanteert, na te kijken. ■

Nu we bewezen hebben wat het minimum gewicht is van $\mathcal{C}_k(n,q)^\perp$ voor q even, is de volgende stap om te proberen deze codewoorden te beschrijven. Hiervoor volgen we de aanpak van Adriaensen uit [1]. Opnieuw bekijken we $k = 1$. We willen dus de kleinste niet ledige even verzamelingen karakteriseren. Voor $n = 2$ zijn dit duidelijk hyperovalen. We concentreren ons voor de karakterisering dan ook op $n \geq 3$. Dit is een open probleem dat in [1] is opgelost voor $q = 4$ en $q = 8$. Ook voor $q = 2$ is dit opgelost in [8] door Bagchi en Inamdar. Dit laatste geval zit echter al in onze bespreking voor $q = p$ priem. Hier focussen we vooral op het resultaat voor $q = 4$ of 8 uit [1]. Daarvoor hebben we het begrip van een hypercilinder nodig. We baseren ons hiervoor op [1, Definition 3.7].

Definitie 3.3.21 (Hypercilinder). Neem een vlak π en een $(n-3)$-ruimte τ die scheef zijn aan elkaar in $\mathrm{PG}(n,q)$, $n \geq 3$. Veronderstel dat $\mathcal{O}$ een hyperovaal is in π. De verzameling bestaande uit de punten $\left(\bigcup_{P\in\mathcal{O}}\langle P,\tau\rangle\right) \setminus \tau$ noemen we een hypercilinder. De deelruimte τ wordt ook de top genoemd en $\mathcal{O}$ de basis. Soms zullen we ook π de basis noemen.

Wanneer we spreken over een hypercilinder in een k-ruimte, bedoelen we steeds dat deze de k-ruimte opspant. We noemen de kleinste niet ledige even verzamelingen vanaf nu minimum even verzamelingen. Het blijkt dat de minimum even verzamelingen altijd een hypercilinder zijn wanneer $q = 2, 4$ en 8 [1]. Als $q = 2$, dan is een hypercilinder hetzelfde als het verschil van twee hypervlakken [1]. We tonen dit aan in het volgende lemma. Deze eigenschap impliceert dat de karakterisering voor q even overeenkomt met deze voor $q = p$ priem waar deze overlappen, i.e. $q = 2$.

Lemma 3.3.22. *Als $q = 2$, dan is een hypercilinder in $\mathrm{PG}(n,q)$ gelijk aan het symmetrisch verschil van twee hypervlakken.*

Bewijs. Veronderstel dat de hypercilinder $\mathcal{H}$ een top τ en basis $\mathcal{O}$ heeft. Het vlak waar $\mathcal{O}$ in ligt, noemen we π. Neem een punt $P \in \pi$ met $P \notin \mathcal{O}$. Aangezien $q = 2$ zijn er in het vlak π exact drie rechten door P. Twee van deze drie rechten bevatten behalve het punt P alleen punten van $\mathcal{O}$. De derde rechte l bevat geen enkel punt van $\mathcal{O}$, omdat $|\mathcal{O}| = 4$. We bewijzen dat het hypervlak

$\langle l, \tau \rangle$ het complement is van de hypercilinder $\mathcal{H}$. Inderdaad de punten van l en τ liggen duidelijk niet in $\mathcal{H}$. Neem een punt Q dat ligt op een rechte door een punt $R' \in l$ en een punt $R \in \tau$. Bij constructie kan Q enkel behoren tot de hypercilinder $\mathcal{H}$ als er een rechte is door Q en een punt S van $\mathcal{O}$ die τ snijdt. Zo'n rechte kan niet bestaan. Inderdaad $\langle \pi, Q \rangle$ is een 3-ruimte die τ snijdt in juist één punt. Dit punt is dan noodzakelijk het punt R. Bijgevolg is de enige rechte door Q die zowel π als τ snijdt de rechte $\langle Q, R \rangle$ en deze bevat geen punten van $\mathcal{O}$. Dus vinden we $Q \notin \mathcal{H}$ en in het bijzonder $\langle l, \tau \rangle \nsubseteq \mathcal{H}$. Op analoge manier ziet men ook in dat elk punt dat niet in $\mathcal{H}$ ligt, bevat is in het hypervlak $\langle l, \tau \rangle$. Hiermee hebben we bewezen dat $\mathcal{H}$ gelijk is aan het complement van een hypervlak, wat gelijk is aan het symmetrisch verschil van twee andere hypervlakken omdat $q = 2$ is. ■

Wanneer q even is, maar $q > 2$, geldt bovenstaande redenering niet meer. De reden is dat we in π meer punten hebben die niet behoren tot $\mathcal{O}$. We kunnen wel alle 0-secanten in π gebruiken om hypervlakken te maken die disjunct zijn aan de hypercilinder $\mathcal{H}$. De doorsnede van deze hypervlakken bevat duidelijk τ. We weten ook dat deze doorsnede hoogstens dimensie $n - 3$ heeft. Anders zou deze een punt gemeen hebben met π en dan gaan alle 0-secanten in π door 1 punt. Dit kan niet door de grootte van $\mathcal{O}$ als $q > 2$. Dus zien we in dat τ gelijk is aan de doorsnede van deze hypervlakken en bijgevolg uniek bepaald door de hypercilinder. Voor $q = 4$ en $q = 8$ tonen we vervolgens aan dat de minimum even verzamelingen hypercilinders zijn. We doen dit door het probleem te herleiden naar de situatie in $\mathrm{PG}(3, q)$ zoals in [1]. Hiervoor bewijzen we eerst de twee volgende stellingen. De eerste stelling is bewezen door Adriaensen, Mannaert, Santonastaso en Zullo in [5].

Stelling 3.3.23. *[5, Theorem 5.7] Beschouw q even. Zij $\mathcal{S}$ een minimum even verzameling waarvoor er minstens één vlak bestaat met exact $(q + 2)$ punten van $\mathcal{S}$. Veronderstel ook dat $\mathcal{S}$ in elke 3-ruimte door een vlak met exact $q + 2$ punten van $\mathcal{S}$ een hypercilinder is, dan is $\mathcal{S}$ een hypercilinder.*

Bewijs. Veronderstel dat π een vlak is zoals in het gegeven: $|\pi \cap \mathcal{S}| = q+2$ en $\mathcal{S}$ kan in elke 3-ruimte door π worden beschreven als een hypercilinder. Voor elke 3-ruimte door π heeft de bijhorende hypercilinder als top een zeker punt T; voor de basis kunnen we telkens π kiezen. We noemen τ de verzameling van alle toppen T. Omdat er door het vlak π in $\mathrm{PG}(n, q)$ juist θ_{n-3} verschillende 3-ruimten gaan, is $|\tau| = \theta_{n-3}$. Merk op dat het niet mogelijk is dat twee verschillende 3-ruimten aanleiding geven tot eenzelfde top, waardoor het tellen van de 3-ruimten voldoende is om de grootte van τ te bepalen. We tonen eerst aan dat τ een deelruimte is. Hieruit volgt immers onmiddellijk dat $\mathcal{S}$ een hypercilinder is met top τ en basis π.

Neem twee verschillende punten T_1 en T_2 van τ. We tonen aan dat de rechte $t = \langle T_1, T_2 \rangle$ volledig bestaat uit punten van τ. Merk op dat $\pi \cap t = \emptyset$, omdat anders $T_2 \in t \subseteq \langle T_1, \pi \rangle$ wat niet kan aangezien $\langle T_1, \pi \rangle$ en $\langle T_2, \pi \rangle$ verschillende 3-ruimten zijn. Neem nu een punt $P \in \pi \cap \mathcal{S}$ en beschouw het vlak $\sigma = \langle P, t \rangle$. Ten eerste merken we op dat, voor $i \in \{1, 2\}$, alle punten van de rechte $\langle T_i, P \rangle$ tot $\mathcal{S}$ behoren behalve T_i, omdat $\langle T_i, \pi \rangle$ een hypercilinder is met top T_i. Vervolgens nemen we door het punt P een rechte l in het vlak σ met $l \neq \langle P, T_i \rangle$, $i \in \{1, 2\}$. Daaropvolgend beschouwen we door l de 3-ruimte $\rho = \langle l, \pi \rangle$. Aangezien ρ een 3-ruimte door π is, bevat deze een hypercilinder met als top een punt T. We bewijzen vanuit het ongerijmde dat T ligt op de rechte l.

Veronderstel dat T niet ligt op de rechte l, dan kunnen we een vlak κ nemen door de rechte l in de 3-ruimte ρ zodat T niet bevat is in het vlak κ. Door l zijn er in ρ immers $q + 1$ verschillende vlakken, waarvan er maar één het punt T bevat. We bepalen vervolgens hoe het vlak κ de verzameling $\mathcal{S}$ snijdt. Omdat $l \cap \pi = P$ en zowel π als κ bevat zijn in de 3-ruimte ρ, heeft het vlak κ een rechte m door P gemeen met π. Aangezien $\pi \cap \mathcal{S}$ een hyperovaal is, heeft de rechte m naast het punt P nog één ander punt gemeen met $\mathcal{S}$. In het bijzonder is dus $\kappa \cap \mathcal{S} \neq \emptyset$ en blijven er nog

twee mogelijkheden over voor $\kappa \cap \mathcal{S}$. Aangezien $\kappa \subseteq \rho$ en $\mathcal{S} \cap \rho$ een hypercilinder is, zijn deze mogelijkheden als volgt: ofwel is $\kappa \cap \mathcal{S}$ het symmetrisch verschil van twee rechten, ofwel is het een hyperovaal. Inderdaad als κ het punt T bevat, dan is $\kappa \cap \mathcal{S}$ duidelijk het symmetrisch verschil van twee rechten, waaronder de rechte $\langle P, T\rangle$. Als $T \notin \kappa$, dan moet κ alle rechten van de hypercilinder snijden en is $\kappa \cap \mathcal{S}$ een hyperovaal. Het is duidelijk dat het eerste geval hier niet mogelijk is omdat per constructie $T \notin \kappa$, dus is $\kappa \cap \mathcal{S}$ een hyperovaal. Aangezien de rechte l het punt P met $\mathcal{S}$ gemeen heeft, is l een 2-secant aan $\mathcal{S}$. Het vlak $\sigma = \langle P, t\rangle$ snijdt het vlak κ in de rechte l. Omdat $\kappa \cap \mathcal{S}$ een hyperovaal is, vormt de doorsnede van $\mathcal{S}$ met de 3-ruimte $\langle \kappa, \sigma\rangle$ een hypercilinder door het gegeven. Dat $\langle \kappa, \sigma\rangle$ een 3-ruimte is, kan men inzien door op te merken dat $\kappa \subseteq \rho$, maar $\sigma \nsubseteq \rho$. We zien opnieuw dat er voor $\sigma \cap \mathcal{S}$ twee mogelijkheden zijn: het symmetrisch verschil van twee rechten of een hyperovaal. Echter hebben we eerder gezien dat de rechten $\langle T_i, P\rangle \subseteq \sigma$, met $i \in \{1, 2\}$, volledig tot $\mathcal{S}$ behoren behalve het punt T_i. Hierdoor is geen enkele van bovenstaande mogelijkheden toepasbaar en vinden we een strijdigheid. We hebben dus bewezen dat $T \in l$.

Dit wil zeggen dat de rechte $\langle P, T\rangle = l$ exact q punten van $\mathcal{S}$ bevat en het punt dat niet bevat is in $\mathcal{S}$ is een punt van τ. Merk op dat l elke rechte door het punt P in het vlak σ kan zijn behalve $\langle T_i, P\rangle \subseteq \sigma$, met $i \in \{1, 2\}$. Maar ook deze laatste twee rechten bevatten q punten van $\mathcal{S}$ en één punt van τ. Dus elke rechte door P in σ bevat q punten van $\mathcal{S}$ en het enige punt dat niet bevat is in $\mathcal{S}$, is de top van een hypercilinder in een 3-ruimte. Vanwege het feit dat er $q + 1$ rechten zijn door P in het vlak σ, vinden we dus $q+1$ punten van τ in σ. Deze $q+1$ punten vormen het complement van een even verzameling en snijden dus elke rechte in σ in een oneven aantal punten. Hierbij gebruiken we dat q even is en elke rechte dus een oneven aantal punten bevat. In het bijzonder vormen deze punten een blokkerende verzameling van grootte $q + 1$ en bijgevolg is dit een rechte. Omdat we al weten dat T_1 en T_2 de rechte t opspannen, is dit noodzakelijk de rechte t. We hebben dus aangetoond dat de rechte t enkel bestaat uit punten van τ wat het bewijs vervolledigt. ■

Stelling 3.3.24. *[1, Proposition 3.9] Stel dat de enige minimum even verzamelingen in* $\mathrm{PG}(3, q)$*, met* q *even, hypercilinders zijn, dan zijn voor alle* $n \geq 3$ *de minimum even verzamelingen in* $\mathrm{PG}(n, q)$ *hypercilinders.*

Bewijs. Stel dat $\mathcal{S}$ een minimum even verzameling is in $\mathrm{PG}(n, q)$. We zullen aantonen dat er een vlak π bestaat zodat $\pi \cap \mathcal{S}$ een hyperovaal is en in elke 3-ruimte door zo'n vlak is $\mathcal{S}$ een hypercilinder. Hierdoor kunnen we de vorige stelling toepassen waaruit volgt dat $\mathcal{S}$ een hypercilinder is. Veronderstel hiervoor dat $n > 3$ en neem een punt $P \in \mathcal{S}$. Er bestaat een rechte door P zodat deze nog exact één extra punt van $\mathcal{S}$ bevat. Inderdaad, aangezien $\mathcal{S}$ een even verzameling is, zou elke rechte door P nog minstens drie extra punten bevatten als dit niet waar is. Omdat dat er θ_{n-1} rechten zijn door het punt P volgt hieruit dat $|\mathcal{S}| \geq 1 + 3\theta_{n-1}$. Dit geeft een strijdigheid met het feit dat $\mathcal{S}$ een minimum even verzameling is. Beschouw dus een rechte l die een 2-secant is aan $\mathcal{S}$. Merk op dat als we $\mathcal{S}$ beperken tot een vlak dat we een even verzameling in dit vlak bekomen. Bijgevolg bevat elk vlak door l minstens $q + 2$ punten van $\mathcal{S}$. We tonen vervolgens aan dat er een vlak π door l bestaat met juist $q + 2$ punten van $\mathcal{S}$. We doen dit opnieuw door te tellen en we gebruiken hierbij dat een even verzameling altijd een even aantal punten bevat. Door de rechte l zijn er θ_{n-2} vlakken en als deze allemaal minstens $q + 2$ extra punten bevatten, vinden we dat $|\mathcal{S}| \geq 2 + \theta_{n-2}(q+2)$. Dit geeft een strijdigheid met het gegeven dat $|\mathcal{S}| = q^{n-2}(q+2)$. Er bestaat dus minstens één vlak waarin $\mathcal{S}$ een hyperovaal is.

Voor het tweede deel van het bewijs nemen we een willekeurig vlak π met $|\pi \cap \mathcal{S}| = q + 2$. De punten van $\mathcal{S}$ vormen een hyperovaal in π. Wanneer we $\mathcal{S}$ beperken tot een 3-ruimte ρ door π, dan is $\mathcal{S}$ nog steeds een even verzameling en dus is $|\rho \cap \mathcal{S}| \geq q(q+2)$. Nu tellen we een laatste keer om het bewijs af te ronden. Er zijn θ_{n-3} verschillende 3-ruimten door π die allemaal minstens $q(q+2)$

punten van $\mathcal{S}$ bevatten. Dit geeft:

$$\begin{aligned} q^{n-2}(q+2) = |\mathcal{S}| &\geq (q+2) + \theta_{n-3}(q(q+2) - (q+2)) \\ &= (q+2) + \theta_{n-3}(q^2+q-2) \\ &= (q+2) + q^{n-1} + 2q^{n-2} - q - 2 = q^{n-2}(q+2). \end{aligned}$$

Deze ongelijkheid is dus een gelijkheid. Dit kan enkel als elke 3-ruimte ρ door π juist $q(q+2)$ punten gemeen heeft met $\mathcal{S}$. Door het gegeven is $\rho \cap \mathcal{S}$ een hypercilinder en kunnen we zoals eerder gezegd de vorige stelling toepassen, wat het bewijs afrondt. ■

We weten nu dat het voldoende is om te bewijzen dat een minimum even verzameling in $\mathrm{PG}(3,q)$ een hypercilinder is in $\mathrm{PG}(3,q)$. Hiervoor blijkt dat het toereikend is om aan te tonen dat elke rechte een 0-, 2- of q-secant is als $q \geq 4$. Merk op dat voor $q = 4$ dit triviaal voldaan is. Daarnaast is het complement van een even verzameling in $\mathrm{PG}(3,4)$ grondig onderzocht in [21] door Hirschfeld en Hubaut en hieruit volgt dat de minimum even verzamelingen in $\mathrm{PG}(3,4)$ hypercilinders zijn [1]. We kunnen dit dus uitbreiden naar $\mathrm{PG}(n,4)$ zoals opgemerkt door Adriaensen in [1].

Stelling 3.3.25. *[13, Proposition 3] Gegeven een even verzameling $\mathcal{S}$ in $\mathrm{PG}(3,q)$, met q even en $q \geq 4$, zodat elke rechte een 0-, 2- of q-secant is aan $\mathcal{S}$. Als $|\mathcal{S}| = q(q+2)$, dan is $\mathcal{S}$ een hypercilinder.*

Zonder bewijs. ■

Later is er in [1] echter een stelling bewezen die aantoont dat het voldoende is dat er één q-secant bestaat aan de minimum even verzameling. Deze stelling zal handiger zijn om de karakterisering voor $q = 8$ aan te tonen. We introduceren eerst de nodige begrippen en lemma's.

Lemma 3.3.26. *[1, Lemma 3.10] Gegeven een vlak π en een rechte $l \subset \pi$ in $\mathrm{PG}(3,q)$, q even, en een even verzameling $\mathcal{S}$. De verzameling $(\pi \cap \mathcal{S}) \triangle l$ is een blokkerende verzameling in π.*

Bewijs. Neem een rechte m in het vlak π. We tonen aan dat deze een oneven aantal punten van de verzameling $(\pi \cap \mathcal{S}) \triangle l$ bevat. Wanneer we het inproduct van de karakteristieke vectoren bekijken, vinden we:

$$\chi_{(\pi\cap\mathcal{S})\triangle l} \cdot \chi_m = \chi_{\pi\cap\mathcal{S}} \cdot \chi_m + \chi_l \cdot \chi_m = \chi_{\mathcal{S}} \cdot \chi_m + 1 = 1.$$

Voor de eerste gelijkheid gebruikten we dat na de gelijkheid de bijdrage van een punt in de doorsnede van $\pi \cap \mathcal{S}$ met l nog steeds 0 is. Inderdaad als dit punt ook tot m behoort, komt deze tweemaal voor in de som. Aangezien q even is en we modulo 2 rekenen, valt deze bijdrage weg. Vervolgens mogen we $\chi_{\pi\cap\mathcal{S}}$ vervangen door $\chi_{\mathcal{S}}$ omdat χ_m coëfficiënt 0 heeft voor punten buiten π. De rechten l en m vallen ofwel samen ofwel snijden ze, dus is $\chi_l \cdot \chi_m = 1 \pmod 2$. Tenslotte gebruikten we dat $\mathcal{S}$ een even verzameling is, waardoor $\chi_{\mathcal{S}} \cdot \chi_m = 0 \pmod 2$. Hiermee hebben we bewezen dat elke rechte minstens één punt bevat van de verzameling $(\pi \cap \mathcal{S}) \triangle l$. ■

Voor de volgende begrippen baseren we ons op [1]. De tweede definitie is in [1] enkel gedefinieerd voor minimum even verzamelingen. Wij geven hier een ruimere definitie opdat we deze later kunnen gebruiken om codewoorden uit te sluiten.

Definitie 3.3.27 (Rédei blokkerende verzameling). Gegeven een blokkerende verzameling $\mathcal{B}$ in $\mathrm{PG}(2,q)$, een punt $P \notin \mathcal{B}$ en een rechte l door het punt P. Wanneer de ongelijkheid $|\mathcal{B} \setminus l| \geq q$ een gelijkheid is, noemen we l een Rédei rechte ten opzichte van $\mathcal{B}$. De verzameling $\mathcal{B}$ wordt dan een Rédei blokkerende verzameling genoemd. Als we de rechten door het punt P bekijkt, zien we in dat de ongelijkheid $|\mathcal{B} \setminus l| \geq q$ waar is.

Definitie 3.3.28 (Rédei rechte t.o.v. een even verzameling). Gegeven een even verzameling $\mathcal{S}$ in $\mathrm{PG}(3,q)$. Een vlak π is een Rédei vlak ten opzichte van $\mathcal{S}$ als er een rechte $l \subset \pi$ bestaat zodat $(\pi \cap \mathcal{S}) \triangle l$ een Rédei blokkerende verzameling is in π met Rédei rechte l ten opzichte van $(\pi \cap \mathcal{S}) \triangle l$. Een equivalente voorwaarde is $|(\pi \cap \mathcal{S}) \setminus l| = q$. We noemen de rechte l een Rédei rechte ten opzichte van $\mathcal{S}$.

Nu we weten wat een Rédei rechte is, kunnen we het laatste lemma aantonen alvorens we overgaan tot de beloofde stelling.

Lemma 3.3.29. *[1, Lemma 3.12] Beschouw een vlak π en een minimum even verzameling $\mathcal{S}$ in $\mathrm{PG}(3,q)$, dan is $|\pi \cap \mathcal{S}| \leq 2q$. Wanneer deze ongelijkheid een gelijkheid is, geldt er voor elk vlak $\rho \neq \pi$ dat de rechte $\pi \cap \rho$ ofwel scheef is aan $\mathcal{S}$, ofwel een Rédei rechte is van ρ ten opzichte van $\mathcal{S}$.*

Bewijs. Als $\mathcal{S} \cap \pi = \emptyset$, dan is de stelling triviaal voldaan. Veronderstel dus dat $\mathcal{S} \cap \pi \neq \emptyset$ en neem een rechte $l \subset \pi$ die minstens één punt van $\mathcal{S}$ bevat. De q vlakken ρ door l verschillend van π bevatten dan ook punten van $\mathcal{S}$. Dankzij het vorige lemma is $(\rho \cap \mathcal{S}) \triangle l$ een blokkerende verzameling in ρ. Zoals eerder opgemerkt is $|(\rho \cap \mathcal{S}) \setminus l| \geq q$ en bij gelijkheid is l een Rédei rechte. Omdat dit geldt voor alle q de vlakken ρ vinden we volgende ondergrens:

$$|\mathcal{S}| = q(q+2) \geq |\mathcal{S} \cap \pi| + q \cdot q.$$

Hieruit volgt onmiddellijk dat $|\pi \cap \mathcal{S}| \leq 2q$. Wanneer dit een gelijkheid is, is l een Rédei rechte ten opzichte van $\mathcal{S}$ voor alle andere vlakken erdoor. Merk op dat dit dan ook geldt voor alle andere rechten in π die een punt van $\mathcal{S}$ bevatten. De rechten in π die geen punt bevatten van $\mathcal{S}$ zijn opgenomen in het eerste geval van de stelling. ■

Stelling 3.3.30. *[1, Proposition 3.13] Als een minimum even verzameling $\mathcal{S}$ in $\mathrm{PG}(3,q)$, met q even, een q-secant bevat, dan is $\mathcal{S}$ een hypercilinder.*

Bewijs. Stel dat de rechte l een q-secant is aan de minimum even verzameling $\mathcal{S}$. Het unieke punt van $l \setminus \mathcal{S}$ noemen we P. Neem een willekeurig vlak π door de rechte l. De verzameling $(\pi \cap \mathcal{S}) \triangle l$ is een blokkerende verzameling in π zoals eerder bewezen en de rechte l bevat juist één punt, P, hiervan. Zoals al meerdere keren opgemerkt bevat de verzameling $(\mathcal{S} \cap \pi) \setminus l$ nog minstens q andere punten van $\mathcal{S}$. Langs de andere kant mogen dit in dit geval hoogstens q punten zijn opdat $|\mathcal{S} \cap \pi| \leq 2q$ en de vorige stelling geldig blijft. Hierdoor is $|(\pi \cap \mathcal{S}) \triangle l| = q+1$. Uit Stelling 2.2.7 volgt dat deze blokkerende verzameling een rechte m is door het punt P. Bijgevolg is $\pi \cap \mathcal{S}$ gelijk aan het symmetrisch verschil van deze rechte m met de rechte l die beide door P gaan. Omdat π representatief is voor elk van de $q+1$ verschillende vlakken door l kunnen we deze redenering herhalen. We bekomen dat $\mathcal{S}$ de unie is van $q+2$ verschillende rechten door het punt P, maar zonder het punt P. Beschouw nu een willekeurig vlak ρ zodat $P \notin \rho$. Dit vlak zal elk van deze $q+2$ rechten snijden in een verschillend punt en dus is $|\rho \cap \mathcal{S}| = q+2$. Bijgevolg is dit een hyperovaal. We kunnen $\mathcal{S}$ dan beschrijven als de hypercilinder met top P en basis ρ. ■

Via deze stelling kunnen we opnieuw makkelijk inzien dat alle minimum even verzamelingen $\mathcal{S}$ in $\mathrm{PG}(3,4)$ hypercilinders zijn. Er zijn namelijk 21 rechten door een punt $P \in \mathcal{S}$, maar $|\mathcal{S}| = 24$. Er bestaat dus juist één 4-secant door P waardoor we de vorige stelling kunnen toepassen. Het bewijs voor $q = 8$ is niet zo eenvoudig. We willen graag gebruiken dat als er geen 8-secanten zijn aan $\mathcal{S}$, dan zijn er ook geen 6-secanten. Voor q even noemen we een rechte l een grote secant aan een even verzameling $\mathcal{S}$ als $|l \cap \mathcal{S}| > \frac{q}{2}$ zoals gedefinieerd in [1] voor minimum even verzamelingen. In [1] wordt bewezen dat een minimum even verzameling die geen hypercilinder is, hoogstens één grote secant rechte bevat. Als deze bestaat, dan zijn er ook bepaalde gevolgen, o.a. het bestaan van een deelveld $\mathbb{F}_s$, $s \neq 2$, van $\mathbb{F}_q$. Wij bewijzen deze stelling hier niet. Zoals de auteur zelf opmerkt

sluiten deze enkel 6-secanten uit voor $q = 8$, maar kan dit ook op een eenvoudigere manier worden bewezen.

Lemma 3.3.31. *In* $\mathrm{PG}(3, 8)$ *geldt er dat een minimum even verzameling* $\mathcal{S}$ *die geen* q*-secant bevat, i.e. een 8-secant, ook geen* 6*-secant bevat.*

Bewijs. Dit bewijs is gebaseerd op [1]. Stel dat er een 6-secant l bestaat aan de minimum even verzameling $\mathcal{S}$ in $\mathrm{PG}(3, 8)$. Er moet een Rédei vlak π door de rechte l, i.e. $|(\mathcal{S} \cap \pi) \setminus l| = q$, bestaan. Stel dat dit niet zo is, dan bevat elk vlak door l minstens $q + 2$ extra punten van $\mathcal{S}$. Merk op dat we hier gebruiken dat $\mathcal{S}$ een even verzameling is en dus moet $|\mathcal{S} \cap \pi|$ even zijn. Ook hebben we eerder al gezien dat $|(\mathcal{S} \cap \pi) \setminus l| \geq q$. Aangezien er zo $q + 1$ vlakken zijn, vinden we volgende ondergrens:

$$q(q + 2) = |\mathcal{S}| \geq 6 + (q + 1)(q + 2).$$

Dit geeft duidelijk een strijdigheid en er bestaat dus minstens één Rédei vlak π door de 6-secant rechte l. De blokkerende verzameling $(\pi \cap \mathcal{S}) \triangle l$ in π heeft derhalve grootte $(9 - 6) + 8 = 11$. Aangezien $\mathcal{S}$ geen q-secanten bevat, bevat deze blokkerende verzameling geen rechte. Volgens [12] van Bruen heeft een blokkerende verzameling in $\mathrm{PG}(2, 8)$ die geen rechten bevat, minstens grootte 12, wat een strijdigheid geeft. ∎

We kunnen nu aantonen dat de minimum even verzamelingen in $\mathrm{PG}(3, 8)$ hypercilinders zijn.

Stelling 3.3.32. *[1, Proposition 3.16] In* $\mathrm{PG}(3, 8)$ *is een minimum even verzameling* $\mathcal{S}$ *een hypercilinder.*

Bewijs. Veronderstel dat $\mathcal{S}$ een minimum even verzameling is in $\mathrm{PG}(3, 8)$, maar geen hypercilinder. Dankzij Stelling 3.3.30 bestaan er dan geen q-secanten, i.e. 8-secanten, aan $\mathcal{S}$. Uit het vorige lemma volgt er dat er ook geen 6-secanten bevat zijn in $\mathcal{S}$. Door een punt $P \in \mathcal{S}$ zijn er bijgevolg enkel 2- of 4-secanten aan $\mathcal{S}$. We noteren dit laatste aantal rechten als x. We tellen vervolgens de punten van $\mathcal{S}$ via de punten op rechten door P. Zo bepalen we wat x is. Er zijn $\theta_2 = 73$ rechten door P. Exact x rechten hiervan bevatten drie extra punten van $\mathcal{S}$, de andere rechten door P leveren één extra punt. Hierdoor vinden we:

$$80 = q(q + 2) = |\mathcal{S}| = 1 + 3x + (73 - x) = 74 + 2x.$$

Er volgt dat $x = 3$. We kunnen elk punt $P \in \mathcal{S}$ toewijzen aan één van de twee volgende verzamelingen. In de eerste verzameling liggen de drie verschillende 4-secanten door P in één vlak; in de tweede verzameling liggen deze drie rechten niet in eenzelfde vlak. In het volgende deel van het bewijs vergaren we wat meer informatie over hoe de vlakken zich verhouden tot de verzameling $\mathcal{S}$.

De vlakken die i punten van $\mathcal{S}$ bevatten, noemen we i-secant vlakken en we noteren hun aantal als m_i, met $i \in \mathbb{N}$. Om geen verwarring te creëren met de rechten gebruiken we vanaf nu i-secant rechten in plaats van enkel het begrip i-secant. Beschouw voor een punt P dat in de eerste verzameling zit, het vlak π dat de drie 4-secant rechten door P bevat. De zes andere rechten door P in π bevatten juist één extra punt van $\mathcal{S}$. Wanneer we de punten van $\mathcal{S} \cap \pi$ tellen via de rechten door P, vinden we $|\mathcal{S} \cap \pi| = 1 + 6 \cdot 1 + 3 \cdot 3 = 16$. Bijgevolg is π een 16-secant vlak. Voor een punt P uit de tweede verzameling zijn er drie vlakken door P die elk twee 4-secanten door P bevatten. Men kan analoog narekenen dat zo'n vlak een 14-secant is. Voor beide verzamelingen geldt dat alle niet besproken vlakken door een punt P hoogstens één 4-secant rechte door P bevatten. Dit zijn dus 10- of 12-secant vlakken. In het bijzonder ligt elk punt $P \in \mathcal{S}$ op hoogstens één 16-secant vlak. We tonen nu eerst aan dat elk punt van $\mathcal{S}$ effectief op een 16-secant vlak ligt. Hiervoor tellen we

op twee manieren de koppels (P, π), met P een punt en π een 14-secant vlak zodat $P \in \mathcal{S} \cap \pi$. Voor de eerste manier beginnen we met de vlakken te tellen. Er zijn m_{14} verschillende 14-secant vlakken en deze bevatten elk 14 punten. Dit geeft aanleiding tot $14m_{14}$ koppels. Voor de tweede wijze tellen we eerst de punten. De punten uit de eerste verzameling liggen niet op een 14-secant vlak zoals eerder besproken. De punten uit de tweede verzameling liggen op drie verschillende 14-secant vlakken. Omdat elk punt uit de eerste verzameling op juist één 16-secant ligt, zijn er $16m_{16}$ punten in de eerste puntenverzameling. De grootte van deze tweede puntenverzameling is dus $(80 - 16m_{16})$. Wanneer we de twee tellingen gelijkstellen, vinden we:

$$14m_{14} = (80 - 16m_{16})3 = 16(5 - m_{16})3.$$

Merk op dat alle factoren uit het rechterlid copriem zijn met de factor 7 uit het linkerlid. Dus moet $m_{14} = 0$ en $m_{16} = 5$ opdat de vergelijking klopt. Als er geen 14-secant vlakken zijn, kunnen er ook geen punten zijn uit de tweede verzameling. Hiermee hebben we bewezen dat elk punt van $\mathcal{S}$ in juist één 16-secant vlak ligt.

De vijf verschillende 16-secant vlakken noteren we als π_i, $i \in \{1, \ldots, 5\}$. Ons doel is onder andere om aan te tonen dat deze vijf vlakken door eenzelfde rechte gaan. We doen dit in verschillende stappen. We noemen een punt $P \in \mathcal{S}$ van type i als $P \in \pi_i$. Beschouw nu de punten P_1 en P_2 die respectievelijk van type 1 en 2 zijn. De rechte door deze twee punten $\langle P_1, P_2 \rangle$ ligt niet in een 16-secant vlak omdat P_1 en P_2 van een verschillend type zijn. Een vlak π door $\langle P_1, P_2 \rangle$ bevat al minstens twee punten van $\mathcal{S}$ en hoogstens één 4-secant rechte door een vast punt van $\mathcal{S}$. Dit is dus een 10-secant of een 12-secant vlak. Stel dat π een 12-secant is. Dit is hetzelfde als veronderstellen dat er één 4-secant rechte l_{π,P_1} gaat door P_1 in π. Deze rechte is dan de doorsnede van π en π_1. We kunnen hetzelfde zeggen over P_2: er gaat één 4-secant rechte l_{π,P_2} door P_2 in π en dit is de doorsnede van π met π_2. Dus snijden de rechten l_{π,P_1} en l_{π,P_2} elkaar in het snijpunt van $\pi \cap \pi_1 \cap \pi_2$. Aangezien er drie verschillende 4-secanten zijn door P_1 vinden we dat er drie mogelijkheden zijn voor het 12-secant vlak π. Bijgevolg zijn er dus ook drie snijpunten van de vorm $\pi \cap \pi_1 \cap \pi_2$. We noemen deze R_1, R_2 en R_3. De rechte $\pi_1 \cap \pi_2$ erdoor noemen we l. Merk op dat deze punten niet afhangen van welk punt P_1 of P_2 we juist kiezen in π_1 en π_2. Hieruit kunnen we afleiden dat elke 4-secant in π_1 en π_2 gaat door één van deze drie punten. De rechte l is de rechte waarvan we zullen aantonen dat elke 16-secant vlak erdoor gaat. Deze informatie samen met speciale eigenschappen van de punten R_1, R_2 en R_3 zal leiden tot de strijdigheid die we zoeken.

De punten R_1, R_2 en R_3 behoren niet tot $\mathcal{S}$ omdat ze zowel in π_1 als π_2 liggen en elk punt van $\mathcal{S}$ is bevat in exact één 16-secant vlak. We bewijzen nu dat R_1, R_2 en R_3 de enige punten zijn in $\pi_1 \setminus \mathcal{S}$ die op meer dan één 4-secant rechte liggen. We doen dit door de grootte van de verzameling

$$\mathcal{V} = \{(l_1, l_2, Q) \mid\mid l_1, l_2 \text{ verschillende 4-secant rechten in } \pi_1, Q = l_1 \cap l_2\}$$

te bepalen op twee manieren. Ten eerste is $|\pi_1 \cap \mathcal{S}| = 16$ en gaan er door elk punt van $\pi_1 \cap \mathcal{S}$ drie verschillende 4-secant rechten. Hieruit volgt dat er $\frac{16 \cdot 3}{4} = 12$ verschillende 4-secanten zijn in π_1. We delen hier door vier omdat we anders elke rechte vier keer tellen. Voor l_1 hebben we dus 12 keuzes en voor l_2 zijn er 11 keuzes. Het snijpunt Q ligt vast éénmaal we deze rechten gekozen hebben. We vinden dus $|\mathcal{V}| = 12 \cdot 11 = 132$. Voor de tweede manier beginnen we met het punt Q te kiezen. Als $Q \in \mathcal{S}$ zijn er 16 opties. Elk zo'n punt ligt op drie verschillende 4-secant rechten. Dit geeft in totaal een bijdrage van $16 \cdot 3 \cdot 2$. Alle twaalf de 4-secanten gaan door één van de punten R_i, met $i \in \{1, 2, 3\}$. Dus ligt elke R_i op vier verschillende 4-secanten in π_1 en geven deze punten een bijdrage van $3 \cdot 4 \cdot 3$ aan $|\mathcal{V}|$. Zo hebben we in totaal een bijdrage van $16 \cdot 3 \cdot 2 + 3 \cdot 4 \cdot 3 = 132$. Dit is gelijk aan de eerder afgeleide grootte van $\mathcal{V}$. Er zijn dus geen andere punten meer die bijdragen aan $|\mathcal{V}|$. In het bijzonder betekent dit dat R_1, R_2 en R_3 inderdaad de enige punten zijn van $\pi_1 \setminus \mathcal{S}$ die op meer dan één 4-secant rechte liggen.

We kunnen alle bovenstaande redeneringen herhalen met P_2 vervangen door een punt van type i, met $i \in \{3,4,5\}$. Dit resulteert in drie punten R_1', R_2' en R_3' die liggen in $\pi_1 \cap \pi_i$ zodat elke 4-secant rechte in π_1 of π_i gaat door één van deze drie punten. Maar omdat in π_1 de punten R_1, R_2 en R_3 de enige punten zijn die niet tot $\mathcal{S}$ behoren en op meerdere 4-secanten liggen, is $\{R_1, R_2, R_3\} = \{R_1', R_2', R_3'\}$. We besluiten dat de vijf 16-secant vlakken allemaal gaan door de rechte $l = \langle R_1, R_2, R_3\rangle$. Omdat elke 4-secant rechte ligt in één van die vijf vlakken, snijdt elke 4-secant rechte de rechte l in één van de punten R_i, met $i \in \{1,2,3\}$. Wanneer we de vlakken door l bekijken, hebben we net bewezen dat er hierbij vijf verschillende 16-secant vlakken zijn. Bijgevolg bevatten de andere vlakken door l geen punten van $\mathcal{S}$ want $|\mathcal{S}| = 80$ en $l \cap \mathcal{S} = \emptyset$. Hieruit halen we ook dat de rechten door R_1 die niet in π_i liggen, $i \in \{1,\dots,5\}$, 0-secant rechten zijn. Daardoor ligt R_1 niet in een 10-secant vlak. Inderdaad in zo'n vlak vormt $\mathcal{S}$ een hyperovaal en zouden er meerdere 2-secanten door R_1 zijn. Nu bekomen we een strijdigheid door de punten $P \in \mathcal{S}$ te tellen via de vlakken π door het punt R_1. Meer concreet voeren we een dubbele telling uit van de koppels (P, π), met $P, R_1 \in \pi$ en $P \in \mathcal{S}$. Ten eerste zijn er door R_1 vijf 16-secant vlakken, deze geven al $5 \cdot 16 = 80$ koppels. Daarnaast zijn er enkel 0-secant vlakken en 12-secant vlakken door R_1. Het aantal van deze laatste soort noteren we als x. De bijdrage hiervan is $12x$. Voor de tweede manier starten we van een willekeurig punt $P \in \mathcal{S}$, zo zijn er 80. Door de rechte $\langle P, R_1\rangle$ zijn er 9 vlakken, en we vinden dus dat er 720 koppels in totaal zijn. Wanneer we deze twee manieren gelijk stellen kunnen we bepalen wat x is:

$$12x + 80 = 720 \Rightarrow x = \frac{640}{12} = \frac{160}{3}.$$

Maar x is geen geheel getal, wat de beloofde strijdigheid is. Onze assumptie dat $\mathcal{S}$ geen hypercilinder is, is dus vals. ■

Het uitbreiden van deze stelling naar grotere q lijkt moeilijk, maar het oogt aannemelijk dat dit wel waar is. Om dit deel af te ronden vatten we in de volgende stelling de resultaten voor de minimum gewicht codewoorden van $\mathcal{C}_k(n,q)^\perp$, met $q \in \{4,8\}$, samen en bepalen we hoeveel er zijn.

Stelling 3.3.33. *[1, Corollary 3.17] Voor $q \in \{4,8\}$ zijn de minimum gewicht codewoorden van $\mathcal{C}_k(n,q)^\perp$ de karakteristieke vectoren van hypercilinders in een $(n-k+1)$-ruimte. Het aantal minimum gewicht codewoorden is*

$$\begin{bmatrix} n+1 \\ k-1 \end{bmatrix}_q \begin{bmatrix} n-k+2 \\ 3 \end{bmatrix}_q \delta(q),$$

met $\delta(q)$ gelijk aan 168 als $q = 4$ en 32 704 als $q = 8$.

Bewijs. Neem een codewoord $c \in \mathcal{C}_k(n,q)^\perp$ met minimum gewicht. Zoals eerder al gebruikt volgt uit Stellingen 3.3.16, 3.3.6 en 3.3.8 dat $\mathrm{supp}(c)$ bevat is in een $(n-k+1)$-ruimte ρ, dat $c \in \mathcal{C}_1(\rho)^\perp$ en dat ook in die code c een codewoord met minimum gewicht is. We weten uit Stelling 3.3.20 dat dit minimum gewicht gelijk is aan $q^{n-k-1}(q+2)$. Dankzij het verband met even verzamelingen volgt er uit bovenstaande bespreking dat $\mathrm{supp}(c)$ een hypercilinder is in ρ met als basis een hyperovaal. In [35] is door Segre bewezen dat elke hyperovaal in $\mathrm{PG}(2,q)$ met $q \leq 8$ regulier is. Dus is hier de hyperovaal die de basis vormt regulier. We besluiten dat c de karakteristieke vector is van een hypercilinder in een $(n-k+1)$-ruimte.

We tonen nu aan hoeveel codewoorden er zijn met minimum gewicht. Het is voldoende om het aantal hypercilinders die een $(n-k+1)$-ruimte opspannen in $\mathrm{PG}(n,q)$ te tellen. Ten eerste zijn er $\begin{bmatrix} n+1 \\ n-k+2 \end{bmatrix}_q$ verschillende keuzes voor een $(n-k+1)$-ruimte in $\mathrm{PG}(n,q)$. Door de dualiteit van

een projectieve ruimte kunnen we dit aantal ook schrijven als $\begin{bmatrix} n+1 \\ k-1 \end{bmatrix}_q$. Vervolgens tellen we het aantal hypercilinders in één $(n-k+1)$-ruimte. Omdat $q > 2$, is de top van een hypercilinder uniek bepaald zoals eerder opgemerkt. In dit geval is de top een $(n-k-2)$-ruimte. Het is geweten dat er $\begin{bmatrix} n-k+2 \\ n-k-1 \end{bmatrix}_q = \begin{bmatrix} n-k+2 \\ 3 \end{bmatrix}_q$ verschillende $(n-k-2)$-ruimten in $\mathrm{PG}(n-k+1,q)$ zijn. Deze geven dus allemaal aanleiding tot een verschillende hypercilinder. Nu moeten we voor elke top een hyperovaal kiezen in een vlak disjunct aan deze top. Merk op dat de keuze van het disjuncte vlak niet van belang is. Het laatste dat we dus moeten tellen is het aantal reguliere hyperovalen in een vlak, dit is de $\delta(q)$ uit het te bewijzen. Uit oefening 6.3 van projectieve meetkunde weten we dat vijf punten waarvan er geen drie collineair zijn op unieke wijze een kegelsnede bepalen. Ook volgt uit deze oefening dat het aantal irreducibele kegelsneden gelijk is aan q^5-q^2. Als $q=4$ en je verwijdert één punt uit een hyperovaal, dan vormen de overblijvende punten een irreducibele kegelsnede. Dit wil zeggen we uit elke hyperovaal zes verschillende kegelsneden kunnen bekomen. Hieruit volgt dat het aantal hyperovalen gelijk is aan het aantal irreducibele kegelsneden gedeeld door zes, i.e. $\frac{4^5-4^2}{6} = 168 = \delta(4)$. Wanneer $q=8$ is een hyperovaal de unie van een kegelsnede en zijn kern. Als we de kern verwijderen vormen de overige negen punten dus opnieuw een unieke kegelsnede. Er zijn dus evenveel hyperovalen als irreducibele kegelsneden en dit aantal is $8^5-8^2 = 32704 = \delta(8)$. Wanneer we nu het aantal $(n-k+1)$-ruimten, het aantal toppen, i.e. $\begin{bmatrix} n-k+2 \\ 3 \end{bmatrix}_q$, en het aantal hyperovalen in een vlak vermenigvuldigen vinden we het gezochte aantal codewoorden. ■

3.3.6. Vergelijking van de ondergrenzen

We hebben verschillende ondergrenzen gezien voor het minimumgewicht van $\mathcal{C}_k(n,q)^\perp$. De drie voornaamste zijn Stellingen 3.3.3, 3.3.11 en 3.3.14. We kunnen ons nu afvragen welke grens de beste is? Hangt dit af van de parameters $q=p^h$, n en k? We beginnen met de grenzen uit Stellingen 3.3.3 en 3.3.11 te vergelijken. De eerste ondergrens is enkel geldig voor $p \geq 7$. In het geval dat $p=7$ zijn beide ondergrenzen gelijk. We tonen nu aan dat als $p>7$, de tweede ondergrens de betere is. Via enkele berekeningen vinden we:

$$\begin{aligned}
& 2\left(\theta_{n-k}\left(1-\frac{1}{p}\right)+\frac{1}{p}\right) > \frac{12\theta_{n-k}+6}{7} \\
\iff & \theta_{n-k}\left(1-\frac{1}{p}\right)+\frac{1}{p} > \frac{6\theta_{n-k}+3}{7} \\
\iff & 7\theta_{n-k}\left(1-\frac{1}{p}\right)+\frac{7}{p} > 6\theta_{n-k}+3 \\
\iff & \theta_{n-k}\left(1-\frac{7}{p}\right)+\frac{7-3p}{p} > 0.
\end{aligned}$$

We substitueren hierin $q=p^h$ en bekomen dat:

$$\begin{aligned}
& \left(\frac{p^{nh-kh+h}-1}{p^h-1}\right)\left(1-\frac{7}{p}\right)+\frac{7-3p}{p} > 0 \\
\iff & \left(p^{nh-kh+h}-1\right)(p-7)+(7-3p)(p^h-1) > 0 \\
\iff & p^{nh-kh+h+1}-p-7p^{nh-kh+h}+7+7p^h-7-3p^{h+1}+3p > 0 \\
\iff & p^{nh-kh+h+1}-7p^{nh-kh+h}-3p^{h+1}+7p^h+2p > 0.
\end{aligned}$$

Deze waarde is het kleinst wanneer p zo klein mogelijk is, i.e. $p = 11$, en de exponent minimaal is, i.e. $k = n - 1$ en $h = 1$. Wanneer we dit substitueren vinden we de waarde 220. Dus is de ondergrens van Stelling 3.3.11 inderdaad de betere ondergrens. Nu kunnen we ons afvragen of we informatie kunnen halen uit Lemma 3.3.1, waarop de eerste ondergrens is gebaseerd, voor de tweede ondergrens. Meer specifiek kunnen we dit lemma gebruiken om te bepalen hoeveel verschillende niet-nul symbolen een codewoord met een bepaald gewicht hoogstens heeft. Veronderstel dat er een codewoord c zou bestaan in $\mathrm{PG}(n, p^h)$, met $p \neq 2$, zodat het gewicht van c gelijk is aan de ondergrens uit Stelling 3.3.11. Wanneer we Lemma 3.3.1 toepassen met $2m = p - 1$, zien we dat de coëfficiënt bij θ_{n-k} dezelfde is als bij de ondergrens. De constante term is $\frac{p-1}{p}$, terwijl deze bij Stelling 3.3.11 gelijk is aan $\frac{2}{p}$. Dit zijn echter allebei getallen tussen 0 en 1 en het gewicht is een geheel getal. We kunnen dit dus voor beide afronden naar 1. Het codewoord c mag dus hoogstens $p - 1$ verschillende niet-nul symbolen bevatten. Dit levert derhalve geen extra informatie op.

We hadden uit Lemma 3.3.1 nog een andere grens buiten Stelling 3.3.3 gehaald die geldig is voor meer waarden van p. Namelijk als $p \neq 2$ kunnen we Stelling 3.3.2 toepassen. Voor $p \geq 7$ is Stelling 3.3.3 duidelijk minstens even goed. Dit is ook logisch omdat we deze informatie gebruiken in het bewijs van Stelling 3.3.3. Bijgevolg is ook Stelling 3.3.11 in dit geval beter dan Stelling 3.3.2. Wanneer $p = 3$ of 5 kan men analoog aan bovenstaande berekeningen nagaan dat ook dan Stelling 3.3.11 beter is dan Stelling 3.3.2.

We vergelijken nu de huidige beste ondergrens 3.3.11 met Stelling 3.3.14. We starten van de hypothese dat Stelling 3.3.11 opnieuw de betere is. Dit geeft:

$$\begin{aligned}
&2\left(\theta_{n-k}\left(1-\frac{1}{p}\right)+\frac{1}{p}\right) > (q+p)q^{n-k-1} \\
\iff &2\left(\theta_{n-k}\left(p-1\right)+1\right) > p(q+p)q^{n-k-1} \\
\iff &2(p-1)(q^{n-k+1}-1)+2(q-1) > p(q+p)(q-1)q^{n-k-1} \\
\iff &2(p-1)q^{n-k+1}-2(p-q) > pq^{n-k+1}+(p^2-p)q^{n-k}-p^2q^{n-k-1} \\
\iff &(p-2)q^{n-k+1}-(p^2-p)q^{n-k}+p^2q^{n-k-1}-2(p-q) > 0.
\end{aligned}$$

We weten dat wanneer $p = 2$ de ondergrens uit Stelling 3.3.14 wordt bereikt. Dit wil zeggen dat de grens uit Stelling 3.3.11 het enkel even goed kan doen. Indien dit het geval is, zou het linkerlid gelijk aan nul moeten zijn. We vullen in dat $p = 2$, dit geeft:

$$-2q^{n-k}+4q^{n-k-1}-4+2q > 0.$$

Hieruit volgt dat voor $q = 2$, beide grenzen samenvallen. Wanneer $q = 2^h$ en $k = n - 1$ vinden we:

$$-2^{h+1}+4-4+2^{h+1} = 0.$$

Zo zien we dat ook in dit geval de grenzen samenvallen. In de andere gevallen wanneer $q = 2^h$, zal de ondergrens uit Stelling 3.3.14 beter zijn. We kunnen ons nu afvragen wat er gebeurt wanneer $p \neq 2$ is. Het linkerlid van de ongelijkheid die we hierboven hadden voor willekeurige p is het kleinste als $k = n - 1$ en als h zo klein mogelijk is. Merk op dat we weten wat het minimum gewicht is als $q = p$. In dit geval zijn beide grenzen gelijk aan dit minimum gewicht. Daarom vullen we eerst $h = 2$ in, i.e. $q = p^2$. Hieruit halen we:

$$\begin{aligned}
&(p-2)p^{2n-2k+2}-(p^2-p)p^{2n-2k}+p^2p^{2n-2k-2}-2(p-p^2) > 0 \\
\iff &p^{2n-2k+3}-3p^{2n-2k+2}+p^{2n-2k+1}+p^{2n-2k}+2p^2-2p > 0.
\end{aligned}$$

Wanneer we vervolgens invullen dat $k = n - 1$, vinden we:

$$\begin{aligned} & p^5 - 3p^4 + p^3 + p^2 + 2p^2 - 2p > 0 \\ \iff & p^5 - 3p^4 + p^3 + 3p^2 - 2p > 0. \end{aligned}$$

De grootste nulwaarde van dit polynoom is 2, dus zo volgt er dat de grens uit Stelling 3.3.11 de betere grens is voor oneven q met $h > 1$. Wanneer men niet weet wat het minimum gewicht is, is het dus aangeraden om te werken met deze ondergrens. Recent hebben De Boeck en Van de Voorde in [16, Corollary 1.5] nieuwe grenzen voor het minimum gewicht bewezen als $q = p^2$, met $p \geq 7$, namelijk:

$$2p^2 - 2p + 5 \leq d(\mathcal{C}_1(2, p^2)^\perp) \leq 2p^2 - p.$$

In dit geval is het beter om deze grens te gebruiken in plaats van de ondergrens uit Stelling 3.3.11, i.e. $2p^2 - 2p + 2$. Daarnaast geven we ter illustratie ook een bovengrens voor het minimum gewicht van $\mathcal{C}_k(n, q)^\perp$. In [24, Corollary 4.15] is door Lavrauw, Storme en Van de Voorde de volgende bovengrens bewezen:

$$d(\mathcal{C}_k(n, q)^\perp) \leq 2q^{n-k} - q^{n-k-1}\frac{(q-p)}{(p-1)}.$$

3.3.7. Alternatief bewijs voor het minimum gewicht van de incidentiecode

We kunnen het verband met k-blokkerende verzamelingen en de ondergrens voor het minimum gewicht van $\mathcal{C}_{n-k}(n, q)^\perp$ gebruiken om op een andere manier het minimum gewicht van $\mathcal{C}_k(n, q)$ te bepalen. We ronden dit hoofdstuk af met de bespreking van dit resultaat van Lavrauw, Storme en Van de Voorde.

Stelling 3.3.34. *[26, Theorem 16] Het minimum gewicht van $\mathcal{C}_k(n, q)$, met $k \geq \frac{n}{2}$ en $p > 7$, is θ_k en een codewoord van gewicht θ_k is een scalair veelvoud van de incidentievector van een k-ruimte.*

Bewijs. Neem een codewoord $c \in \mathcal{C}_k(n, q)$ met minimum gewicht. Als $k \geq \frac{n}{2}$, dan weten we dat ofwel $(c, \rho) = 0$ voor alle $(n-k)$-ruimten ρ ofwel $(c, \rho) \neq 0$ voor alle $(n-k)$-ruimten ρ. In het eerste geval is $c \in \mathcal{C}_{n-k}(n, q)^\perp$, waarvan het minimum gewicht minstens $\frac{12\theta_k+6}{7}$ is. Zo'n codewoord kan dus nooit aanleiding geven tot het minimum gewicht, want we weten al dat er codewoorden bestaan met gewicht θ_k. Als $(c, \rho) \neq 0$ en $w(c) \leq \theta_k$, dan weten we uit Stelling 3.1.5 dat $\mathrm{supp}(c)$ een minimale k-blokkerende verzameling is. Uit Stelling 2.2.7 weten we dat een k-blokkerende verzameling waarvan de grootte hoogstens θ_k is, een k-deelruimte is. Hieruit volgt dan het te bewijzen. ∎

4 Code van punten en deelruimten

4.1. Gewichten van codewoorden uitsluiten

In dit hoofdstuk bestuderen we meer in detail de code $\mathcal{C}_k(n,q)$. Het eerste wat we zullen doen is aantonen dat er onder bepaalde voorwaarden geen codewoorden zijn met gewicht in het open interval $]\theta_k, 2q^k[$. We volgen hiervoor de aanpak van Lavrauw, Storme, Sziklai en Van de Voorde uit [22]. We bewijzen eerst enkele andere stellingen die we zullen nodig hebben.

Lemma 4.1.1. *[22, Lemma 10] In* $\mathrm{PG}(n,q)$*, met* $q = p^h$*,* $h \geq 1$ *en* $p > 2$*, geldt er voor twee kleine minimale* k*-blokkerende verzamelingen* $\mathcal{B}_1$ *en* $\mathcal{B}_2$ *dat* $\mathcal{B}_1 - \mathcal{B}_2 \in \mathcal{C}_{n-k}(n,q)^\perp$*.*

Bewijs. Aangezien elke $(n-k)$-ruimte τ juist $1 \pmod p$ punten gemeen heeft met $\mathcal{B}_i$, $i \in \{1,2\}$, dankzij Stelling 2.2.9 volgt er dat $(\mathcal{B}_i, \tau) = 1$. Hieruit weten we dat $(\mathcal{B}_1 - \mathcal{B}_2, \tau) = 0$ voor alle $(n-k)$-ruimten τ, dus hebben we wat we moesten bewijzen: $\mathcal{B}_1 - \mathcal{B}_2 \in \mathcal{C}_{n-k}(n,q)^\perp$. ■

Lemma 4.1.2. *[22, Lemma 11] Voor een codewoord* $c \in \mathcal{C}_k(n,q)$ *met gewicht kleiner dan* $2q^k$ *geldt er dat als er een* $(n-k)$*-deelruimte* ρ *bestaat zodat* $(c,\rho) \neq 0$*, dan heeft* $\mathrm{supp}(c)$ *met elke kleine minimale* $(n-k)$*-blokkerende verzameling* $\mathcal{B}$ *precies* $1 \pmod p$ *punten gemeen.*

Bewijs. Neem een codewoord $c \in \mathcal{C}_k(n,q)$ met gewicht kleiner dan $2q^k$ en zodat er een $(n-k)$-deelruimte ρ bestaat waarvoor $(c,\rho) \neq 0$. Dankzij het vorige lemma weten we dat voor alle kleine minimale $(n-k)$-blokkerende verzamelingen $\mathcal{B}_1$ en $\mathcal{B}_2$ geldt dat $(c, \mathcal{B}_1 - \mathcal{B}_2) = (c,\mathcal{B}_1) - (c,\mathcal{B}_2) = 0$. Daaruit volgt dat $(c,\mathcal{B})$ dezelfde constante is voor alle kleine minimale $(n-k)$-blokkerende verzamelingen $\mathcal{B}$. Daarnaast weten we uit Stelling 3.1.5 dat c als coördinaten enkel waarden 0 of a heeft, met $a \in \mathbb{F}_p^*$. Daardoor leiden we af dat $(c,\mathcal{B}) = a(\mathrm{supp}(c),\mathcal{B})$ en daaropvolgend dat $(\mathrm{supp}(c),\mathcal{B})$ ook een constante modulo p is. Nu is het voldoende om een goede $(n-k)$-blokkerende verzameling te kiezen waarvoor we weten dat $(\mathrm{supp}(c),\mathcal{B}) = 1 \pmod p$. Kies een $(n-k)$-ruimte τ, dan is τ een kleine minimale $(n-k)$-blokkerende verzameling zoals besproken in het deel over de inleidende begrippen. Dankzij Stelling 3.1.5 vinden we dat $(\mathrm{supp}(c),\tau) = 1 \pmod p$ en dus geldt er voor elke kleine minimale $(n-k)$-blokkerende verzameling $\mathcal{B}$ dat $(\mathrm{supp}(c),\mathcal{B}) = 1 \pmod p$. ■

We kunnen nu de codewoorden die niet bevat zijn in de duale code uitsluiten onder bepaalde voorwaarden.

Stelling 4.1.3. *[22, Theorem 12] De code* $\mathcal{C}_k(n,q) \setminus \mathcal{C}_{n-k}(n,q)^\perp$*, met* $p > 5$*,* $h \geq 1$*, heeft geen codewoorden met gewicht in het open interval* $]\theta_k, 2q^k[$*.*

Bewijs. Beschouw een codewoord $c \in \mathcal{C}_k(n,q) \setminus \mathcal{C}_{n-k}(n,q)^\perp$ en veronderstel dat $\mathrm{supp}(c) = \mathcal{S}$ hoogstens $2q^k - 1$ punten bevat. We zullen aantonen dat $\mathcal{S}$ een k-ruimte is en bijgevolg $|\mathcal{S}| = \theta_k$, wat de stelling bewijst. We gebruiken hiervoor de theorie rond lineaire k-blokkerende verzamelingen. Neem een willekeurige lineaire kleine minimale $(n-k)$-blokkerende verzameling $\mathcal{B}$. We weten dat $\mathcal{B}$ per definitie correspondeert met de verzameling $\bar{\mathcal{B}} = \mathcal{B}(\bar{\tau})$ bestaande uit de $(h-1)$-ruimten van de Desarguesiaanse spread $\mathcal{D}$ die een $h(n-k)$-ruimte $\bar{\tau}$ in $\mathrm{PG}((n+1)h-1,p)$

snijden. Ook hebben we uit Stelling 3.1.5 dat $\mathcal{S}$ een minimale k-blokkerende verzameling is, omdat $c \notin \mathcal{C}_{n-k}(n,q)^{\perp}$. Daarnaast volgt er uit deze stelling ook dat $\mathcal{S}$ elke $(n-k)$-ruimte snijdt in $1 \pmod p$ punten en dan krijgen we uit Lemma 2.2.8 dat $\mathcal{S}$ een kleine k-blokkerende verzameling is. Via veldreductie correspondeert $\mathcal{S}$ met een deelverzameling $\bar{\mathcal{S}}$ van de $(h-1)$-spread $\mathcal{D}$ in $\mathrm{PG}((n+1)h-1,p)$. Dankzij Lemma 4.1.2 weten we dat $\mathcal{S}$ en $\mathcal{B}$ juist $1 \pmod p$ punten gemeen hebben. Bijgevolg hebben $\bar{\mathcal{S}}$ en $\bar{\mathcal{B}}$ juist $1 \pmod p$ spread elementen gemeen of anders gezegd er snijden $1 \pmod p$ spread elementen van $\bar{\mathcal{S}}$ de deelruimte $\bar{\tau}$. Echter aangezien elke $h(n-k)$-ruimte $\bar{\tau}$ in $\mathrm{PG}((n+1)h-1,p)$ een kleine minimale lineaire $(n-k)$-blokkerende verzameling bepaalt en $\mathcal{B}$ willekeurig was, kunnen we zeggen dat elke $h(n-k)$-ruimte exact $1 \pmod p$ spread elementen van de verzameling $\bar{\mathcal{S}}$ snijdt. We noteren de punten van de deelruimten uit $\bar{\mathcal{S}}$ als $\tilde{\mathcal{S}}$, merk op dat $\tilde{\mathcal{S}}$ een $(h(k+1)-1)$-blokkerende verzameling is in $\mathrm{PG}(h(n+1)-1,p)$. We tonen nu eerste enkele eigenschappen aan van $\tilde{\mathcal{S}}$.

Elk spread element van $\bar{\mathcal{S}}$ dat een $h(n-k)$-ruimte snijdt, doet dit in $1 \pmod p$ punten omdat dit deelruimten zijn. Aangezien $\mathcal{S}$ een minimale k-blokkerende verzameling is, zijn er $1 \pmod p$ spread elementen die een $h(n-k)$-ruimte snijden. Dus zal ook $\tilde{\mathcal{S}}$ elke $h(n-k)$-ruimte snijden in $1 \pmod p$ punten. Daarnaast kunnen we ook de grootte van $\tilde{\mathcal{S}}$ begrenzen via Lemma 2.2.8 toegepast op $\mathcal{S}$:

$$|\tilde{\mathcal{S}}| = |\mathcal{S}|\frac{p^h-1}{p-1} < \frac{3(p^{hk}-p^{hk-1})}{2}\left(\sum_{i=0}^{h-1} p^i\right) = \frac{3(p^{h(k+1)-1}-p^{hk-1})}{2} < \frac{3(p^{h(k+1)-1}+1)}{2}.$$

Dus is $\tilde{\mathcal{S}}$ een kleine $(h(k+1)-1)$-blokkerende verzameling in $\mathrm{PG}(h(n+1)-1,p)$, meer nog het zal blijken dat $\tilde{\mathcal{S}}$ ook minimaal is. Neem hiervoor een punt $\bar{R} \in \tilde{\mathcal{S}}$. Het spread element van $\bar{S}$ waarin $\bar{R}$ ligt noemen we $\bar{\rho}$ en het corresponderende punt in $\mathrm{PG}(n,q)$ noteren we als R. De k-blokkerende verzameling $\mathcal{S}$ is minimaal in $PG(n,q)$, dus is er door R een $(n-k)$-ruimte σ die raakt aan $\mathcal{S}$ in het punt R. We weten dat σ correspondeert met een $(h(n-k+1)-1)$-ruimte $\bar{\sigma}$ in $\mathrm{PG}(h(n+1)-1,p)$. Er geldt dan dat $\bar{\rho}$ het enige spread element van $\bar{\mathcal{S}}$ is dat $\bar{\sigma}$ snijdt. Omdat $\dim(\bar{\rho}) = h-1$, kunnen we dus door $\bar{R}$ een $h(n-k)$-ruimte in $\bar{\sigma}$ construeren die enkel $\bar{R}$ gemeen heeft met $\tilde{\mathcal{S}}$. Aangezien $\bar{R}$ willekeurig was, hebben we aangetoond dat $\tilde{\mathcal{S}}$ minimaal is. Nu we dit weten kunnen we Stelling 2.2.9 toepassen op $\tilde{\mathcal{S}}$, hierdoor heeft elke deelruimte $1 \pmod p$ of 0 punten gemeen met $\tilde{\mathcal{S}}$. Bijgevolg is elke rechte scheef, rakend of volledig bevat in $\tilde{\mathcal{S}}$, dus is $\tilde{\mathcal{S}}$ een deelruimte. Voor een bewijs van deze eigenschap verwijzen we naar [43, Lemma 2.1.3], de bachelorproef van de auteur. Aangezien $\tilde{\mathcal{S}}$ elke $h(n-k)$-ruimte snijdt in $\mathrm{PG}(h(n+1)-1,p)$, moet $\dim(\tilde{\mathcal{S}}) \geq h(k+1)-1$ zijn. Maar $\tilde{\mathcal{S}}$ bevat hoogstens $\frac{3(p^{h(k+1)-1}+1)}{2}$ punten en er geldt dat $\frac{p^{h(k+1)}-1}{p-1} \leq \frac{3(p^{h(k+1)-1}+1)}{2} \leq \frac{p^{h(k+1)+1}-1}{p-1}$, dus is $\dim(\tilde{\mathcal{S}}) = h(k+1)-1$ en $\tilde{\mathcal{S}}$ is een $(h(k+1)-1)$-ruimte. Hieruit volgt onmiddellijk dat de spread elementen van $\bar{\mathcal{S}}$ dezelfde $(h(k+1)-1)$-ruimte opspannen en via veldreductie vinden we dat $\mathcal{S}$ een k-ruimte is in $\mathrm{PG}(n,q)$ wat we wilden aantonen. ∎

Via deze stelling en de eerder afgeleide ondergrens voor het minimum gewicht van $\mathcal{C}_k(n,q)^{\perp}$ kunnen we dan het volgende resultaat afleiden:

Stelling 4.1.4. *[22, Theorem 14] Als $p = 7$ zijn er geen codewoorden in $\mathcal{C}_k(n,q)$ met gewicht in het open interval $]\theta_k, \frac{12\theta_k+2}{7}[$. Als $p > 7$ zijn er geen codewoorden met gewicht in het open interval $]\theta_k, \frac{12\theta_k+6}{7}[$.*

Bewijs. Als $p > 7$, dan is het minimum gewicht van $\mathcal{C}_k(n,q)^\perp$ minstens $\frac{12\theta_k+6}{7}$ dankzij Stelling 3.3.3. Voor $p = 7$, bewees deze stelling dat dit gewicht minstens $\frac{12\theta_k+2}{7}$ is. We kunnen dus Stelling 4.1.3 toepassen om aan te tonen dat de codewoorden waarvan het gewicht zou liggen in de intervallen uit het gegeven niet bestaan. ∎

In onze vergelijking van de verschillende ondergrenzen hebben we echter gezien dat Stelling 3.3.11 een betere ondergrens is voor het minimum gewicht van $\mathcal{C}_k(n,q)^\perp$. We kunnen bovenstaand resultaat dus verbeteren:

Stelling 4.1.5. *Als $p > 5$ zijn er geen codewoorden in $\mathcal{C}_k(n,q)$ met gewicht in het open interval*

$$\left]\theta_k, 2\left(\theta_k\left(1-\frac{1}{p}\right)+\frac{1}{p}\right)\right[.$$

We kunnen in sommige gevallen dit interval verder uitbreiden. Hiervoor hebben we eerst nog de volgende hulpstelling nodig. We hadden eerder al een karakterisering gezien van de codewoorden in $\mathcal{C}_k(n,q) \cap \mathcal{C}_k(n,q)^\perp$ als $k \geq \frac{n}{2}$. We zullen deze hiervoor gebruiken.

Stelling 4.1.6. *[22, Corollary 16] Als $k \geq \frac{n}{2}$, dan is $\mathcal{C}_k(n,q) \setminus \mathcal{C}_k(n,q)^\perp = \mathcal{C}_k(n,q) \setminus \mathcal{C}_{n-k}(n,q)^\perp$.*

Bewijs. Uit Stelling 3.1.3 weten we dat als $k \geq \frac{n}{2}$, dan is een codewoord $c \in \mathcal{C}_k(n,q)$ ook bevat in $\mathcal{C}_k(n,q)^\perp$ als en slechts als $(c,\rho) = 0$ voor alle deelruimten ρ met dimensie minstens $n-k$. Als $c \in \mathcal{C}_k(n,q)^\perp$, volgt hieruit onmiddellijk dat ook $c \in \mathcal{C}_{n-k}(n,q)^\perp$. Stel nu dat $c \in \mathcal{C}_{n-k}(n,q)^\perp$. Dankzij Stelling 3.1.1 weten we dat (c,ρ) een constante b is voor alle deelruimten ρ met dimensie minstens $n-k$. Merk op dat $b = 0$ omdat $c \in \mathcal{C}_{n-k}(n,q)^\perp$. Dankzij Stelling 3.1.3 vinden we dan dat $c \in \mathcal{C}_k(n,q)^\perp$. ∎

Stelling 4.1.7. *[22, Corollary 19] De code $\mathcal{C}_{n-1}(n,q)$, met $q = p^h$, $h \geq 1$, $p > 5$, heeft geen codewoorden met gewicht in het open interval $]\theta_{n-1}, 2q^{n-1}[$.*

Bewijs. Dankzij Stelling 4.1.3 weten we dat er geen codewoorden zijn van $\mathcal{C}_{n-1}(n,q) \setminus \mathcal{C}_1(n,q)^\perp$ met gewicht in $]\theta_{n-1}, 2q^{n-1}[$. Echter Stelling 4.1.6 impliceert dat

$$\mathcal{C}_{n-1}(n,q) \setminus \mathcal{C}_1(n,q)^\perp = \mathcal{C}_{n-1}(n,q) \setminus \mathcal{C}_{n-1}(n,q)^\perp$$

en we weten ook uit Stelling 3.2.5 dat het minimum gewicht van $\mathcal{C}_{n-1}(n,q) \cap \mathcal{C}_{n-1}(n,q)^\perp$ gelijk is aan $2q^{n-1}$. Dus heeft in totaal $\mathcal{C}_{n-1}(n,q)$ geen codewoorden met gewicht in dit interval, waaruit het te bewijzen volgt. ∎

Stelling 4.1.8. *[22, Corollary 21] De code $\mathcal{C}_k(n,p)$, met $p > 5$, heeft geen codewoorden met gewicht in het open interval $]\theta_k, 2p^k[$.*

Bewijs. Uit Stelling 4.1.3 volgt dat de code $\mathcal{C}_k(n,p) \setminus \mathcal{C}_{n-k}(n,p)^\perp$ geen codewoorden met gewicht in $]\theta_k, 2p^k[$ heeft. Echter in Stelling 3.3.18 is bewezen dat het minimum gewicht van $\mathcal{C}_{n-k}(n,p)^\perp$ gelijk is aan $2p^k$, waardoor $\mathcal{C}_k(n,p) \cap \mathcal{C}_{n-k}(n,p)^\perp$ ook geen codewoorden heeft met gewicht in dit interval. Hieruit volgt dan wat we wilden bewijzen. ∎

De stellingen die we hierboven hebben afgeleid zijn een verbetering van het eerdere artikel [26] van Lavrauw, Storme en Van de Voorde. Hierin proberen ze ook aan te tonen dat het interval van codewoorden met gewicht in $]\theta_k, 2q^k[$ leeg is. Ze beperken hun daar tot het geval dat $k \geq \frac{n}{2}$, omdat je dan de doorsnede van $\mathcal{C}_k(n,q) \cap \mathcal{C}_k(n,q)^\perp$ kan karakteriseren. Opnieuw door gebruik te maken van het verband met blokkerende verzamelingen kunnen ze de volgende stellingen aantonen die we hier geven zonder bewijs.

Stelling 4.1.9. *[26, Theorem 7] Als $k \geq \frac{n}{2}$, dan is de incidentievector van een kleine niet triviale lineaire k-blokkerende verzameling geen codewoord van $\mathcal{C}_k(n,q)$.*

Stelling 4.1.10. *[26, Corollary 2] Als $k \geq \frac{n}{2}$, dan zijn de codewoorden c van $\mathcal{C}_k(n,q)$ met gewicht in $]\theta_k, 2q^k[$ waarvoor er een $(n-k)$-ruimte ρ bestaat met $(c,\rho) \neq 0$, scalaire veelvouden van niet-lineaire minimale k-blokkerende verzamelingen.*

De auteurs van [26] wijzen ook op het feit dat er een conjectuur is dat elke kleine minimale k-blokkerende verzameling lineair is. Als dit waar is dan volgt uit bovenstaande Stelling 4.1.10 hetzelfde als Stelling 4.1.3 op voorwaarde dat $k \geq \frac{n}{2}$. Ook is er in [26] aangetoond dat als $q = p^2$, met $p > 11$, we opnieuw codewoorden kunnen uitsluiten door te steunen op Stelling 4.1.10. Voor $q = p^3$, $p \geq 7$, is er eveneens aangetoond dat bovenstaande conjunctuur waar is door Lavrauw, Storme en Van de Voorde in [23] en voor $k = n-1$ door Harrach, Metsch, Szőnyi en Weiner in [19].

Stelling 4.1.11. *[26, Corollary 3] Als $k \geq \frac{n}{2}$, dan zijn er geen codewoorden $c \in \mathcal{C}_k(n,p^2) \backslash \mathcal{C}_k(n,p^2)^\perp$, met $p > 11$, waarvan het gewicht ligt in het open interval $]\theta_k, 2p^{2k}[$.*

Stelling 4.1.12. *Als $k \geq \frac{n}{2}$, dan zijn er geen codewoorden $c \in \mathcal{C}_k(n,p^3) \setminus \mathcal{C}_k(n,p^3)^\perp$, met $p \geq 7$, waarvan het gewicht ligt in het open interval $]\theta_k, 2p^{3k}[$.*

Er zijn verdere classificatie resultaten bewezen door Adriaensen en Denaux in [2] en [3]. Voor voldoende grote q wordt in [2] gekeken naar codewoorden tot gewicht ruwweg $3q^k$. Als q ook niet priem is, gaat men in [3] tot gewicht ruwweg $\sqrt{q}q^k$. De resultaten in deze publicaties gaan meer algemeen over de codes $\mathcal{C}_{j,k}(n,q)$. We zullen deze kort bespreken in deel 6.1. In de volgende paragraaf bekijken we in meer detail de veel bestudeerde code $\mathcal{C}_{n-1}(n,q)$.

4.2. De incidentiecode van punten en hypervlakken

We weten al wat het minimum gewicht is van $\mathcal{C}_{n-1}(n,q)$. Ook hebben we gezien dat als $p > 5$ er geen codewoorden zijn met gewicht in $]\theta_{n-1}, 2q^{n-1}[$. We geven nu een alternatieve manier om op een korte en elegante manier alle codewoorden van $\mathcal{C}_{n-1}(n,q)$ die een gewicht hebben dat kleiner is dan $2q^{n-1}$ te karakteriseren voor alle q. We volgen hierbij de aanpak van Adriaensen in [1]. Het originele bewijs van de karakterisering tot en met het gewicht $2q^{n-1}$ door Polverino en Zullo vindt men in [34]. Eerst hebben we nog enkele hulpstellingen nodig.

Lemma 4.2.1. *Als $q > 2$, dan is $\sum_{\alpha \in \mathbb{F}_q} \alpha = 0$.*

Bewijs. We weten dat het polynoom $X^q - X$ als wortels alle $\alpha \in \mathbb{F}_q$ heeft. Hieruit volgt dat:

$$X^q - X = \prod_{\alpha \in \mathbb{F}_q} (X - \alpha) = X^q - \left(\sum_{\alpha \in \mathbb{F}_q} \alpha \right) X^{q-1} + \cdots - X.$$

Als $q > 2$, dan is $q - 1 > 1$, dus komt de term X^{q-1} niet voor in het linkerlid. Dit kan enkel als $\sum_{\alpha \in \mathbb{F}_q} \alpha = 0$. ∎

Lemma 4.2.2. *Beschouw a en b, met $a, b \in \mathbb{F}_p^*$ en $a + b \neq 0$. Dan is elk element van $\mathbb{F}_p^*$ van de vorm $a + \lambda b$, met $\lambda \in \mathbb{N}$.*

Bewijs. Merk op dat $|\mathbb{F}_p^*| = p - 1$, als we dus kunnen aantonen dat $a + \lambda b$ aanleiding geeft tot $p - 1$ verschillende getallen modulo p is de stelling bewezen. Stel dat $a + \lambda b = a + \mu b \pmod p$ met $\lambda, \mu \in \mathbb{N}$.

$$a + \lambda b = a + \mu b \pmod p \iff (\lambda - \mu)b = 0 \pmod p \iff \lambda = \mu \pmod p$$

In de laatste stap hebben we gebruikt dat b^{-1} bestaat omdat $b \in \mathbb{F}_p^*$. Het is duidelijk dat er p verschillende $\lambda \in \mathbb{N}$ zijn modulo p en dat juist één hiervan aanleiding tot $a + \lambda b = 0 \pmod p$. Bijgevolg bestaan er $p - 1$ verschillende getallen van de vorm $a + \lambda b \in \mathbb{F}_p^*$. ■

Voor de volgende stelling hebben we het begrip feet nodig.

Definitie 4.2.3 (Feet van P t.o.v. $\mathcal{A}$). [1, Definition 4.1] Gegeven een punt P en een verzameling van punten $\mathcal{A}$, dan definiëren we de feet van P met respect tot $\mathcal{A}$ als de punten $R \in \mathcal{A}$ zodat:

$$\langle P, R\rangle \cap (\mathcal{A} \setminus \{P\}) = \{R\}.$$

Als $P \notin \mathcal{A}$, dan zijn de feet van P net de punten die op een raaklijn aan $\mathcal{A}$ liggen door P. Als $P \in \mathcal{A}$, dan zijn het de punten die op een 2-secant aan $\mathcal{A}$ liggen door P. Nu we dit begrip beter begrijpen kunnen we overgaan naar de volgende stelling.

Stelling 4.2.4. *[1, Lemma 4.2] Veronderstel dat $c \in \mathcal{C}_{n-1}(n, q)$, met $q > 2$. Voor een willekeurig punt P geldt er dat de feet van P met betrekking tot* $\mathrm{supp}(c)$ *een deelruimte opspannen waar P niet in bevat is.*

Bewijs. Neem een codewoord $c \in \mathcal{C}_{n-1}(n, q)$ en een punt P. Als P slechts nul of één feet heeft met betrekking tot $\mathrm{supp}(c)$, is de stelling geldig. Daarom gaan we er vanuit dat P minstens twee feet heeft. We bewijzen de stelling vanuit het ongerijmde. Stel dat P wel bevat is in de deelruimte voortgebracht door de feet van P. Beschouw de deelverzameling punten $R_0, \ldots, R_k$, met $k \geq 1$, van de feet van P met respect tot de verzameling $\mathrm{supp}(c)$, zodat dit de kleinste deelverzameling is waarvoor $P \in \langle R_0, \ldots, R_k\rangle$. We kunnen zelfs onderstellen dat $k \geq 2$, want als $k = 1$ dan $P \in \langle R_0, R_1\rangle$. Dit kan echter niet omdat R_0 en R_1 feet zijn ten opzichte van P, dus is $k \geq 2$. We weten dat er lineair onafhankelijke vectoren $e_0, \ldots, e_k$ in $V(n + 1, q)$ bestaan zodat:

$$P = \langle e_0\rangle,\ R_1 = \langle e_1\rangle,\ \ldots,\ R_k = \langle e_k\rangle \text{ en } R_0 = \langle e_0 + e_1 + \cdots + e_k\rangle.$$

De span van alle codewoorden van $\mathcal{C}_{n-1}(n, q)$ over $\mathbb{F}_q$ noteren we als C'. Er geldt duidelijk dat $c \in C'$. Het doel is om nu een vector v te maken in $C'^{\perp}$, die niet orthogonaal kan zijn met c, wat een strijdigheid geeft. We definiëren de coördinaten v_Q, $Q \in \mathrm{PG}(n, q)$, van v als volgt:

$$v_Q = \begin{cases} a & \text{als } Q = \langle ae_0 + e_i\rangle \text{ met } 1 \leq i \leq k, \\ -a & \text{als } Q = \langle ae_0 + e_1 + \cdots + e_k\rangle, \\ 0 & \text{anders.} \end{cases}$$

De verzameling $\mathrm{supp}(v)$ bestaat uit de punten op de rechten $l_i = \langle P, R_i\rangle$, met $i = 0, \ldots, k$, behalve de punten $\{P, R_1, \ldots, R_k, R_0'\}$ met $R_0' = \langle e_1 + \cdots + e_k\rangle$. Merk op dat dit punten zijn met $a = 0$ in de gevallen opsplitsing, behalve het punt P. We nemen nu een willekeurig hypervlak π om te controleren of $v \in C'^{\perp}$. Als $P \in \pi$, dan geldt voor elke rechte l_i dat deze ofwel in π ligt ofwel het hypervlak π snijdt in het punt P. We hebben dat $v_P = 0$ en dankzij Lemma 4.2.1 weten we ook dat $\sum_{Q \in l_i} v_Q = \sum_{\alpha \in \mathbb{F}_p} \alpha = 0$. Bijgevolg is $(v, \pi) = 0$. In het geval dat $P \notin \pi$ snijdt elke rechte l_i het hypervlak π in exact één punt. Een rechte l_i, met $i \neq 0$, snijdt het hypervlak in het punt

$\langle a_i e_0 + e_i \rangle$, met $a_i \in \mathbb{F}_p$. Het punt $\langle (a_1 + \cdots + a_k)e_0 + e_1 + \cdots + e_k \rangle$ ligt dan ook in π en dit punt moet het unieke snijpunt zijn van de rechte l_0 met π. Dit punt heeft als coördinaat in v de waarde $-(a_1 + \cdots + a_k)$, voor de andere punten is de coördinaat a_i. Er volgt dat:

$$(v, \pi) = a_1 + \cdots + a_k + -(a_1 + \cdots + a_k) = 0,$$

en dus $v \in C'^{\perp}$. Maar we hebben niet dat $(v, c) = 0$. Inderdaad laten we de supports vergelijken. We weten dat $\mathrm{supp}(v) = \left(\bigcup_{i=0}^{k} l_i\right) \setminus \{P, R_1, \ldots, R_k, R'_0\}$ en dat $\mathrm{supp}(c) \cap (l_i \setminus \{P\}) = \{R_i\}$ door de definitie van de feet van P met respect tot $\mathrm{supp}(c)$. Bijgevolg is $\mathrm{supp}(c) \cap \mathrm{supp}(v) = \{R_0\}$. Omdat $v_{R_0} = -1$ en $c_{R_0} \neq 0$ is $(c, v) = c_{R_0} \cdot v_{R_0} = -c_{R_0} \neq 0$, wat een strijdigheid geeft. We besluiten dat P nooit bevat is in de deelruimte opgespannen door zijn feet met respect tot $\mathrm{supp}(c)$. ■

We kunnen nu de beloofde karakterisering bewijzen.

Stelling 4.2.5. *[1, Theorem 4.4] Gegeven een codewoord $c \in \mathcal{C}_{n-1}(n, q)$ zodat $0 < w(c) \leq 2q^{n-1}$. Als $q > 2$, dan geldt één van de volgende mogelijkheden:*

- $c = a\chi_\pi$, *dus* $w(c) = \theta_{n-1}$,
- $c = a(\chi_\pi - \chi_\rho)$, *dus* $w(c) = 2q^{n-1}$,

met π en ρ verschillende hypervlakken in $\mathrm{PG}(n, q)$ en $a \in \mathbb{F}_p^*$.

Bewijs. Beschouw een codewoord c zoals in het gegeven en we noteren $\mathrm{supp}(c)$ als $\mathcal{S}$. We definiëren b zoals in Stelling 3.1.1 toegepast op het codewoord c, i.e. $b = (c, \rho)$ voor elke deelruimte ρ met dimensie minstens één. Er zijn twee mogelijkheden: ofwel is $b \neq 0$ ofwel is $b = 0$.

Geval 1 ($b \neq 0$): Veronderstel dat $b \neq 0$, we definiëren m als volgt:

$$m = \max\{|S \cap \pi| \; || \pi \text{ een hypervlak in } \mathrm{PG}(n, q)\}.$$

Het doel is om aan te tonen dat $m = \theta_{n-1}$. Hieruit volgt immers dat $\mathcal{S}$ een hypervlak π bevat. We tonen aan dat $\mathcal{S}$ dan gelijk is aan dit hypervlak. Voor een willekeurig punt $P \in \pi$ hebben we dat $c_P = b$. Inderdaad, stel dat dit niet waar zou zijn, dan moet elke rechte door P buiten π nog minstens één ander punt bevatten van $\mathcal{S}$. Omdat er zo $\theta_{n-1} - \theta_{n-2} = q^{n-1}$ rechten zijn, zou er volgen dat $w(c) \geq |\pi| + q^{n-1} = \theta_{n-1} + q^{n-1} > 2q^{n-1}$, wat niet kan door het gegeven. Stel nu dat er een punt P bestaat zodat $P \in \mathcal{S}$, maar $P \notin \pi$. Elke rechte l door P snijdt π in juist één punt R. We weten echter dat $c_R = b$ en $(c, l) = b$, dus moet l nog een derde punt van $\mathcal{S}$ bevatten. Hieruit vinden we opnieuw dat c een te groot gewicht zou hebben: aangezien er θ_{n-1} rechten zijn door P vinden we dat $w(c) \geq 1 + 2\theta_{n-1}$, wat niet kan. We hebben dus bewezen dat als $m = \theta_{n-1}$, dan is $\mathcal{S} = \pi$, en bijgevolg $c = b\chi_\pi$. We kunnen het geval $b \neq 0$ dan ook afronden als we aantonen dat $m = \theta_{n-1}$. We bewijzen dit vanuit het ongerijmde.

Veronderstel dat $m < \theta_{n-1}$ en neem een m-secant hypervlak π en een punt $P \in \pi \setminus \mathcal{S}$. We bekijken het aantal punten van $\mathcal{S}$ op rechten door P. Merk op dat elke rechte door P een punt van $\mathcal{S}$ zal bevatten omdat $b \neq 0$. De rechten door P die bevat zijn in π geven in totaal aanleiding tot m punten van $\mathcal{S}$. Het aantal raaklijnen aan $\mathcal{S}$ door P buiten π noteren we als x. Aangezien er q^{n-1} rechten zijn door P buiten π en de niet raaklijnen hiervan minstens twee punten van $\mathcal{S}$ moeten bevatten, vinden we dat:

$$2q^{n-1} \geq w(c) \geq m + x + (q^{n-1} - x)2 = m - x + 2q^{n-1}.$$

Hieruit volgt onmiddellijk dat $x \geq m$. Dankzij Lemma 4.2.4 weten we dat er een hypervlak τ bestaat waar P niet in ligt, maar de feet van P met respect tot $\mathcal{S}$ wel. Omdat $P \notin \mathcal{S}$, zijn deze feet net de punten die op een raaklijn door P liggen. Daaruit volgt dat $x \leq m$, dus is $x = m$ en bovenstaande ongelijkheid is een gelijkheid. Er geldt dat τ de m feet van P bevat en geen enkel ander extra punt van $\mathcal{S}$. We weten ook dat er geen enkel punt van de feet kan liggen in π, omdat we anders geen gelijkheid hebben in bovenstaande vergelijking. Hieruit zien we dat $\pi \cap \tau \cap \mathcal{S} = \emptyset$. Als $n \geq 3$, dan is $\dim(\pi \cap \tau) \geq 1$, dus moet $(c, \pi \cap \tau) = b = 0$. Dit geeft een strijdigheid met het feit dat $b \neq 0$ en dus is $m = \theta_{n-1}$ als $n \geq 3$. Als $n = 2$, dan is $m > 2$, want anders is S een boog. Maar uit Stelling 2.2.13 volgt dat er altijd een rechte bestaat die disjunct is aan de boog, wat hier niet kan omdat $b \neq 0$. Aangezien $n = 2$, impliceert bovenstaande vergelijking, die een gelijkheid is, dat P op één m-secant π ligt, $m = x$ raaklijnen en $q - m$ verschillende 2-secanten. Dit geldt echter voor elk punt $P \notin \mathcal{S}$, die op een m-secant ligt. In het bijzonder dus ook voor het punt $\pi \cap \tau$ dat niet in $\mathcal{S}$ bevat is zoals eerder aangetoond. Maar zowel π als τ zijn m-secanten, wat een strijdigheid geeft. Dus we hebben dat $m = \theta_{n-1}$, wat dit geval vervolledigt.

Geval 2 $(b = 0)$**:** We willen op een gelijkaardige manier als hiervoor te werk gaan. Daarom definiëren we de verzameling $\mathcal{A}$ als de verzameling van niet-nul coëfficiënten c_P, $P \in \mathcal{S}$, van het codewoord c. Voor elke $a \in \mathcal{A}$, definiëren we:

$$m_a = \max\{|\mathcal{S} \cap \pi| \;||\; \pi \text{ een hypervlak in } \mathrm{PG}(n, q) \text{ zodat } \exists P \in \pi : c_P = a\}.$$

Veronderstel nu dat $m_a \geq m_{-a}$ voor een $a \in \mathcal{A}$. Merk op dat we m_{-a} gelijk aan 0 stellen als $-a \notin \mathcal{A}$. Beschouw een m_a-secant hypervlak π die het punt P bevat met $c_P = a$. Zoals in het vorige geval tellen we de punten van $\mathcal{S}$ op rechten door P, let echter op dat hier wel $P \in \mathcal{S}$. Alle rechten door P die liggen in π geven aanleiding tot m_a punten van $\mathcal{S}$. Ook hebben we dat $b = 0$, dus bestaan er geen raaklijnen door P aan $\mathcal{S}$. Hier noteren we het aantal 2-secanten door P buiten π als x en we vinden dat:

$$2q^{n-1} \geq w(c) \geq m_a + x + (q^{n-1} - x)2 = m_a - x + 2q^{n-1}.$$

Merk op dat P hier meegeteld is in m_a, en we voor een 2-secant dus nog één extra punt in $\mathcal{S}$ moeten tellen en voor alle andere rechten hebben we minstens twee extra punten. Er volgt onmiddellijk dat $x \geq m_a$. Zoals voordien kunnen we opnieuw Stelling 4.2.4 toepassen zodat de feet van P met respect tot $\mathcal{S}$ in een hypervlak τ liggen en $P \notin \tau$. Nu is $P \in \mathcal{S}$, dus zijn de feet van P de punten die op een 2-secant aan $\mathcal{S}$ liggen. Aangezien $b = 0$, vinden we voor elk punt R op een 2-secant l met P dat $c_R = -a$ opdat $(c, l) = 0$. Uit het feit dat we minstens x zo'n punten R hebben en dat deze liggen in het hypervlak τ, volgt er dat $x \leq m_{-a} \leq m_a$. Dit geeft samen met de eerdere ongelijkheid dat $x = m_{-a} = m_a$. We weten dat τ hoogstens m_{-a} punten bevat en minstens x feet, dus volgt er dat $\tau \cap \mathcal{S}$ enkel de $m_{-a} = x$ feet van P bevat. De ongelijkheid bovenaan is ook een gelijkheid omdat $x = m_a$. Hierdoor mag er geen enkel punt van de x feet van P in het hypervlak π liggen. Derhalve hebben we dat $\pi \cap \tau \cap \mathcal{S} = \emptyset$. We zien ook dat er door P juist $m_a = x$ verschillende 2-secanten en $q^{n-1} - m_a$ verschillende 3-secanten zullen gaan buiten π opdat de ongelijkheid een gelijkheid is. We splitsen nu het bewijs op in q even en oneven. Stel dat q even is, dan zijn er geen 3-secanten l aan $\mathcal{S}$. Inderdaad dan zou $0 = b = (c, l) = 1$ omdat we 3 niet-nul getallen optellen modulo 2, wat een strijdigheid geeft. Bijgevolg is $m_a = q^{n-1}$ en zijn τ en π twee q^{n-1}-secant hypervlakken met een lege intersectie. Hieruit kunnen we besluiten dat $\mathcal{S} = \pi \triangle \tau$ en $c = a(\chi_\pi - \chi_\tau)$. We hebben het geval q even bewezen en nemen voor het vervolg aan dat q oneven is.

Alle punten met coëfficiënt $-a$ moeten liggen in $\tau \cup \pi$, want buiten deze deelruimten zijn er enkel 3-secanten l door P maar deze kunnen geen punt met coëfficiënt $-a$ bevatten omdat $c_P = a$ en $(c, l) = 0$. Aangezien $m_a = m_{-a}$, kunnen we het vorige argument herhalen met het punt P vervangen door een punt $R \in \tau$ met $c_R = -a$. Hieruit besluiten we dat er een m_a-secant hypervlak

π' bestaat zodat alle punten met coëfficiënt a liggen in $\tau \cup \pi'$. Echter hebben we eerder bewezen dat alle punten in τ coëfficiënt $-a$ hebben, dus liggen alle punten met coëfficiënt a in π'. Merk op dat er ook minstens $x = m_a$ punten bestaan met coëfficiënt a, dus bevat π' enkel punten met coëfficiënt a. Aangezien a willekeurig is, hebben we bewezen dat voor elke $a \in \mathcal{A}$ er een m_a-secant hypervlak π_a bestaat dat alle punten met coëfficiënt a bevat en enkel deze punten van $\mathcal{S}$. Tenslotte bewijzen we dat $\mathcal{A} = \{a, -a\}$ voor een zekere constante $a \in \mathbb{F}_p$. We weten dat als $a \in \mathcal{A}$, dan is ook $-a \in \mathcal{A}$. Stel dat er nog een ander getal d is dat bevat is in $\mathcal{A}$. Neem dan een punt P met $c_P = d$, hiervoor geldt er dat $P \notin \pi_a \cup \pi_{-a}$. Bijgevolg geldt er voor elke rechte l door P en een punt R van $\pi_a \cap \mathcal{S}$ dat dit een 3-secant is opdat $(c, l) = 0$. Als we het derde punt Q noemen, dan hebben we dat $0 = (c, l) = a + d + c_Q$. Dus is $c_Q = -a - d$, en omdat dit geldt voor elk punt R vinden we dat $m_{a+d} = m_{-a-d} \geq m_a$ voor alle a en $d \in \mathcal{A}$. Door dit nu toe te passen op a en $a + d$, vinden we $m_{a+2d} = m_{-a-2d} \geq m_{a+d} \geq m_a$. Inductief krijgen we in het bijzonder dat $a + \lambda d \in \mathcal{A}$, $\forall \lambda \in \mathbb{N}$. Aangezien elk element in $\mathbb{F}_p^*$ kan worden geschreven als $a + \lambda d$, met $\lambda \in \mathbb{N}$, zie Lemma 4.2.2, vinden we dat $\mathcal{A} = \mathbb{F}_p^*$. Vermits $m_a = m_{a+dp}$, is m_e hetzelfde voor alle $e \in \mathcal{A}$. Echter vinden we dan hieruit en uit de gelijkheid die we in het begin hebben afgeleid dat $2q^{n-1} = w(c) = |\mathcal{A}| m_a = (p-1)m_a$. Maar $p - 1$ is copriem met $q^{n-1} = p^{nh-h}$, dus volgt er $(p-1)|2$. Dit kan enkel als $p = 3$, dus is $\mathcal{A} = \mathbb{F}_p^* = \{1, -1\}$ wat we wilden bewijzen. Indien $p \neq 3$, betekent dit er geen d kan bestaan. Dus in het algemeen kunnen we besluiten dat $\mathcal{A} = \{a, -a\}$ en $2q^{n-1} = w(c) = 2m_a$. Aldus is $m_a = q^{n-1}$ en omdat $\pi_a \cap \pi_{-a} \cap \mathcal{S} = \emptyset$ vinden we dat:

$$c_P = \begin{cases} a & \text{als } P \in \pi_a, \\ -a & \text{als } P \in \pi_{-a}, \\ 0 & \text{anders.} \end{cases}$$

We kunnen dus besluiten dat in dit geval $c = a(\chi_{\pi_a} - \chi_{\pi_{-a}})$. ■

Enkel het geval $q = 2$ ontbreekt in deze classificatie, maar dit geval is apart besproken in [1]:

Stelling 4.2.6. *[1, Lemma 4.5] De codewoorden van $\mathcal{C}_{n-1}(n, 2)$ zijn de nulvector $\mathbf{0}$, de vector bestaande uit allemaal énen $\mathbf{1}$, of van de vorm χ_π of $\chi_\pi - \chi_\rho$ met π en ρ hypervlakken.*

Bewijs. Bij definitie bevat $\mathcal{C}_{n-1}(n, q)$ de codewoorden χ_π met π een hypervlak. Hieruit volgt dat er codewoorden zijn van de vorm $\chi_\pi - \chi_\rho = \chi_\pi + \chi_\rho$, voor de gelijkheid gebruiken we dat $q = 2$. Door χ_π op te tellen bij zichzelf vinden we het codewoord $\mathbf{0}$. Wanneer we alle codewoorden χ_π optellen, vinden we het codewoord $\mathbf{1}$. Omdat de incidentievectoren van hypervlakken de code $\mathcal{C}_{n-1}(n, q)$ voortbrengen, moeten we nu enkel nog controleren dat voor een codewoord c zoals in de stelling beschreven, geldt dat $c + \chi_\sigma$, met σ een hypervlak, opnieuw van één van die vier soorten codewoorden is:

- $c = \mathbf{0}$: $c + \chi_\sigma = \mathbf{0} + \chi_\sigma = \chi_\sigma$.
- $c = \chi_\pi$: $c + \chi_\sigma = \chi_\pi + \chi_\sigma = \chi_\pi - \chi_\sigma$.
- $c = \chi_\pi - \chi_\rho$: Merk op dat $\chi_\pi - \chi_\rho = \chi_{\pi \triangle \rho}$. Er is maar één ander hypervlak τ door $\pi \cap \rho$ en dit is het complement van $\pi \triangle \rho$, dus is $\chi_\pi - \chi_\rho = \mathbf{1} - \chi_\tau$. Wanneer we deze "rekenregel" tweemaal toepassen volgt er dat $c + \chi_\sigma = \mathbf{1} - \chi_\tau + \chi_\sigma = \mathbf{1} + \mathbf{1} - \chi_{\sigma'} = \chi_{\sigma'}$, met σ' het hypervlak dat het complement is van $\tau \cap \sigma$.
- $c = \mathbf{1}$: $c + \chi_\sigma = 1 + \chi_\sigma = \chi_\pi - \chi_\tau$, hiervoor hebben we opnieuw bovenstaande rekenregel toegepast met τ en π twee hypervlakken zodat σ het complement is van $\pi \triangle \tau$.

■

Het blijkt dus dat we voor $q = 2$ de code $\mathcal{C}_{n-1}(n, q)$ volledig kunnen beschrijven. Recent zijn er verdere classificatie resultaten aangetoond voor de code $\mathcal{C}_{n-1}(n, q)$, met $q = p^h$. We geven hier een overzicht van deze artikels gebaseerd op [3]. Specifiek voor het vlak hebben Szőnyi en Weiner in [40] de classificatie resultaten uitgebreid. In [4] bewijzen Adriaensen, Denaux, Storme en Weiner voor q groot genoeg dat alle codewoorden van $\mathcal{C}_{n-1}(n, q)$ met gewicht hoogstens ruwweg $4q^{n-1}$ lineaire combinaties zijn van hypervlakken door eenzelfde $(n-3)$-ruimte. Denaux en Bartoli tonen in [9] aan dat voor q niet priem en voldoende groot, een codewoord $c \in \mathcal{C}_{n-1}(n, q)$ met gewicht hoogstens ruwweg $\frac{q^{n-1}}{2^{n-2}}\sqrt{q}$ een lineaire combinatie is van $\left\lceil \frac{w(c)}{\theta_{n-1}} \right\rceil$ hypervlakken. In het proefschrift van Denaux [17] zijn enkele verbeteringen van deze classificatie bewezen. De reden dat men voor q priem minder ver is geraakt tot nu toe is het bestaan van een "raar" codewoord in dit geval, dat de zaken bemoeilijkt [17]. De meest recente classificatie resultaten staan in [2] en [3] van Adriaensen en Denaux over de algemenere codes $\mathcal{C}_{j,k}(n, q)$. Deze hebben we eerder al kort vermeld en bespreken we in deel 6.1. Eerst bespreken in het volgende hoofdstuk de codewoorden van de duale code van punten en deelruimten voor q even.

5 Duale code van punten en deelruimten

5.1. Gewichten van codewoorden voor q even

Uit Hoofdstuk 3 weten we dat enkel in bepaalde gevallen het minimum gewicht van $\mathcal{C}_k(n,q)^\perp$ gekend is. Als q priem is, hebben we gezien wat het minimum gewicht is. Het blijkt dat in dit geval $\mathcal{C}_k(n,q)^\perp \subseteq \mathcal{C}_k(n,q)$ [7]. Zoals eerder opgemerkt is er geweten wat de codewoorden zijn van $\mathcal{C}_k(n,q)$ tot ruwweg gewicht $3q^k$ voor q voldoende groot. Men kan deze karakterisering uitbreiden naar $\mathcal{C}_k(n,q)^\perp$ door te controleren welke van deze codewoorden behoren tot $\mathcal{C}_k(n,q)^\perp$. In dit deel concentreren we ons op de code $\mathcal{C}_k(n,q)^\perp$ met q even. In Stelling 3.3.20 bewezen we dat deze code minimum gewicht $q^{n-k-1}(q+2)$ heeft. We tonen in onderstaande stelling aan dat elk codewoord in deze code een even gewicht heeft. Dit is een toepassing van [32, Proposition 7] van Pepe, Storme en Van de Voorde.

Stelling 5.1.1. *Beschouw de code $\mathcal{C}_k(n,q)^\perp$ met q even. Als $c \in \mathcal{C}_k(n,q)^\perp$, dan is $w(c)$ een even getal.*

Bewijs. Dit bewijs is gebaseerd op de redenering uit [32, Proposition 7]. Beschouw een codewoord $c \in \mathcal{C}_k(n,q)^\perp$. We noteren $\mathrm{supp}(c)$ als $\mathcal{S}$. Het idee is om op twee manieren de koppels (P,τ), met P een punt en τ een k-ruimte waarvoor geldt dat $P \in \tau \cap \mathcal{S}$, te tellen. Voor de eerste telling starten we met de punten te bekijken. Er zijn $|\mathcal{S}|$ punten mogelijk voor P en die liggen elk in $\begin{bmatrix} n \\ k \end{bmatrix}_q$ verschillende k-ruimten. Zo vinden we dat er $|\mathcal{S}| \begin{bmatrix} n \\ k \end{bmatrix}_q$ koppels zijn. Langs de andere kant weten we dat elke k-ruimte τ een even aantal punten van $\mathcal{S}$ moet bevatten opdat $(c,\tau) = 0$, want q is even. Dit wil zeggen dat uit de tweede telling volgt dat het aantal koppels even is. Dit betekent dat

$$|\mathcal{S}| \begin{bmatrix} n \\ k \end{bmatrix}_q = |\mathcal{S}| \frac{(q^n-1)\cdots(q^{n-k+1}-1)}{(q^k-1)\cdots(q-1)}$$

even is. Merk op dat we van alle factoren behalve $|\mathcal{S}|$ weten dat deze oneven zijn. Hieruit volgt dat $|\mathcal{S}| = w(c)$ even is, wat we wilden bewijzen. ∎

Uit deze stelling blijkt dat het kleinst mogelijke gewicht van een codewoord, verschillend van het minimum gewicht en nul, minstens $q^{n-k-1}(q+2)+2$ is. Wij zullen hier aantonen dat als $q = 8$ en $k \in \{1,\ldots,n-2\}$ een codewoord met gewicht $q^{n-k-1}(q+2)+2$ niet kan bestaan. Voor $q = 4$ zullen we partiële resultaten bekomen. Een alternatieve manier om deze resultaten te vinden is misschien via Stelling 5.1.2 van McEliece. Het is mogelijk dat hieruit volgt dat de gewichten van de codewoorden deelbaar zijn door vier. Een nadeel van deze methode is dat steeds meer berekeningen nodig zijn voor grotere q en n en dat deze moeten worden uitgevoerd voor elke combinatie van de parameters n, k en q. Wij zullen deze berekening niet uitvoeren, maar geven hieronder wat meer informatie rond deze stelling. In [29] heeft McEliece een deelbaarheidsvoorwaarde bewezen waaraan de gewichten van $\mathcal{C}_k(n,q)^\perp$ moeten voldoen. We passen dit resultaat toe zoals in [21]:

Stelling 5.1.2. *[29] Beschouw een codewoord c van de code $\mathcal{C}_k(n,q)^\perp$, met $q = p^h$, dan is het gewicht van c een veelvoud van p^a, met $a = \frac{b}{p-1} - 1$ waarin b het kleinste aantal wortels van de pariteitscontrole veelterm is zodat hun product één is.*

Eigenlijk bewijst McEliece een stelling voor cyclische codes. We mogen dit resultaat toepassen omdat de code $\mathcal{C}_k(n,q)$ een cyclische code is [2]. De duale code is dan ook een cyclische code. We bewijzen dit hier niet, maar we geven wel de nodige definities om Stelling 5.1.2 te begrijpen gebaseerd op [27] en [28] van MacWilliams en Sloane. In de bespreking hieronder gaan we er vanuit dat we telkens werken met een lineaire code over $\mathbb{F}_2$.

Definitie 5.1.3 (Cyclische code). Beschouw de code $\mathcal{C}$ met lengte N. Deze code is cyclisch als voor elk codewoord $c = (c_0, c_1, \ldots, c_{N-1}) \in \mathcal{C}$, geldt dat ook $(c_{N-1}, c_0, \ldots, c_{N-2})$ een codewoord is van de code $\mathcal{C}$.

Stel dat $\mathcal{C}$ een cyclische code is met lengte N. We kunnen met elk codewoord $(c_0, c_1, \ldots, c_{N-1}) \in \mathcal{C}$ de veelterm $c_0 + c_1X + \cdots + c_{N-1}X^{N-1}$ associëren. Er geldt dan dat:

$$\begin{aligned} X(c_0 + c_1X + \cdots + c_{N-1}X^{N-1}) &= c_0X + c_1X^2 + \cdots + c_{N-1}X^N \\ &= c_{N-1} + c_0X + \cdots + c_{N-2}X^{N-1} \pmod{X^N - 1}. \end{aligned}$$

We mogen de lineaire cyclische code $\mathcal{C}$ dus identificeren met een deelverzameling van de verzameling veeltermen:

$$\{f_0 + f_1X + \cdots + f_{N-1}X^{N-1} \pmod{(X^N - 1)}\}.$$

Stel dat de code $\mathcal{C}$ naast lengte N, dimensie K heeft. Er bestaat een unieke veelterm $g(X)$ met graad $N - K$ zodat

$$\mathcal{C} = \{m(X)g(X) \mid\mid m(X) \in \mathbb{F}_q[X],\ \deg m(X) \leq K - 1\}.$$

We noemen $g(X)$ de generator veelterm. Aangezien de duale code $\mathcal{C}^\perp$ ook een lineaire cyclische code is, heeft deze op zijn beurt ook een generator veelterm. Men kan controleren dat deze graad K heeft. De generator veelterm van $\mathcal{C}$ noemt men de pariteitscontrole veelterm voor de code $\mathcal{C}^\perp$. Om Stelling 5.1.2 toe te passen willen we weten wat de wortels van dit polynoom zijn. Men zou deze kunnen bepalen op dezelfde manier als Hirschfeld en Hubaut in [21]. Ze gebruiken daar o.a. het resultaat van McEliece en onderstaand resultaat over de wortels van de pariteitsconrtole veelterm om de even verzamelingen in $\mathrm{PG}(3,4)$ te beschrijven. We introduceren zoals in [21] eerst een begrip: het h-gewicht van een getal met betrekking tot een priemgetal.

Definitie 5.1.4. Het h-gewicht $w_h(a)$ met betrekking tot het priemgetal p van een getal a is gelijk aan r wanneer $a = a_0 + \cdots + a_r$ en

- $a_0 \geq 0$,
- $a_i > 0$ en a_i is een veelvoud van $p^h - 1$ voor $1 \leq i \leq r$,
- Als $a_i = \sum_j b_{i,j}p^j$, met $0 \leq b_{i,j} < p$, dan $\sum_i b_{i,j} < p$,
- r is het grootste getal zodat bovenstaande voorwaarden voldaan zijn.

We geven nu de stelling voor het bepalen van de wortels van de pariteitscontrole veelterm zonder bewijs. Voor meer details hierover verwijzen we de lezer naar [33] van Peterson en Weldon.

Stelling 5.1.5. *[33] Veronderstel dat α een primitieve wortel is van $\mathbb{F}_{q^{n+1}}$, met $q = p^h$, en kies $\beta = \alpha^{q-1}$. De wortels van de pariteitscontrole veelterm van de code $\mathcal{C}_k(n,q)$ zijn β^m met $1 \leq m \leq \frac{(q^{n+1}-1)}{q-1} - 1$ en $w_h(m(q-1)) \leq k$ met betrekking tot p.*

Zoals eerder gezegd kan men deze stellingen proberen gebruiken om onze onderzoeksresultaten op een alternatieve manier te bekomen. Wij gebruiken hieronder een andere aanpak. Merk op dat onze bewijzen niet $k = n - 1$ bestuderen, want hierover zijn al resultaten gekend. Inderdaad, voor de code $\mathcal{C}_{n-1}(n,q)^\perp$, met q even, is de classificatie van de codewoorden met gewicht kleiner dan $q + \sqrt[3]{q^2} + 1$ bewezen door De Boeck in [14]. We geven deze hier zonder bewijs.

Stelling 5.1.6. *[14, Theorem 5.3] Beschouw een codewoord $c \in \mathcal{C}_{n-1}(n,q)^\perp$ met $w(c) \leq q + \sqrt[3]{q^2} + 1$ en q even.*

- *Als q een kwadraat is en $q \geq 64$, dan zijn er twee mogelijkheden voor c. Ofwel is c de incidentievector van een verzameling in een 3-dimensionale Baer deelmeetkunde $\mathcal{B}$ zodat de beperking van c tot de punten van $\mathcal{B}$ een codewoord is van $\mathcal{C}_1(3,\sqrt{q})^\perp$. Ofwel is c de incidentievector van een even verzameling in een vlak van $\mathrm{PG}(n,q)$.*
- *Als q geen kwadraat is of $q \in \{4, 16\}$, dan is c de incidentievector van een even verzameling in een vlak van $\mathrm{PG}(n,q)$.*

Via verder onderzoek is het misschien mogelijk om deze stelling verder te verbeteren en bepaalde gewichten uit te sluiten. Bijvoorbeeld alle even verzamelingen voor $q = 4$ in het vlak zijn gekend. Een samenvatting van deze voor $q = 4$ vindt men in [30]. Maar nog niet voor alle q zijn de even verzamelingen in $\mathrm{PG}(2,q)$ geclassificeerd. Wij zullen ons echter concentreren op $k \in \{1, \ldots, n-2\}$. We bekijken eerst $k = n-2$ en zullen dan uitbreiden naar kleinere k. We beperken ons tot $q = 4$ of 8 omdat we dan kunnen gebruiken dat de codewoorden met minimum gewicht hypercilinders zijn. De eerste stap is om de support $\mathcal{S}$ van een codewoord $c \in \mathcal{C}_{n-2}(n,q)^\perp$ met gewicht $q(q+2)+2$ in te sluiten in een zo klein mogelijke deelruimte.

Stelling 5.1.7. *Gegeven $q = 4$ of 8 en een codewoord $c \in \mathcal{C}_{n-2}(n,q)^\perp$. Als $w(c) = q(q+2)+2$, dan is $\mathrm{supp}(c)$ ofwel een even verzameling van grootte $q(q+2)+2$ in $\mathrm{PG}(3,q)$, ofwel is $\mathrm{supp}(c)$ bevat in een 4-ruimte ρ en bestaat er een punt $R \notin \mathrm{supp}(c)$ in ρ zodat de projectie vanuit R een hypercilinder in een 3-ruimte is.*

Bewijs. Stel dat $c \in \mathcal{C}_{n-2}(n,q)^\perp$ en $w(c) = q(q+2)+2$. We noteren de support van het codewoord c als $\mathcal{S}$. Merk op dat $n \geq 3$ opdat de code anders niet gedefinieerd is. Als $n = 3$, dan is de stelling onmiddellijk voldaan. We kunnen dus veronderstellen dat $n \geq 4$. We baseren ons op het idee uit [26, Theorem 11], hier is dit Stelling 3.3.16. Veronderstel dat $\dim(\langle \mathcal{S} \rangle) \geq 4$. We willen de negatie van Lemma 3.3.15 toepassen. Dit mag, want het besluit van dit lemma is niet waar. Inderdaad, de ongelijkheid:

$$\begin{aligned} |\mathcal{S}| < \theta_3 &\iff q^2 + 2q + 2 < q^3 + q^2 + q + 1 \\ &\iff 0 < q^3 - q - 1 \end{aligned}$$

is correct voor $q \geq 2$. Er bestaat dus een punt $R \in \mathrm{PG}(n,q) \setminus \mathcal{S}$ zodat R ligt op minstens één raaklijn en minstens één secant aan $\mathcal{S}$. Hier bedoelen we met secant een secant rechte. Wanneer we het codewoord c vanuit het punt R projecteren op een hypervlak dat R niet bevat, vinden we een nieuw codewoord $c' \in \mathcal{C}_{n-3}(n-1,q)^\perp$. Het codewoord c' is niet het nulcodewoord, want R ligt op een raaklijn. Maar we verliezen wel minstens één punt van $\mathcal{S}$ bij het projecteren van de secant waar R op ligt. We vatten de situatie als volgt samen:

$$0 < w(c') \leq w(c) - 1 = d(\mathcal{C}_{n-3}(n-1,q)^\perp) + 1.$$

Er zijn 3 mogelijkheden voor $w(c')$:

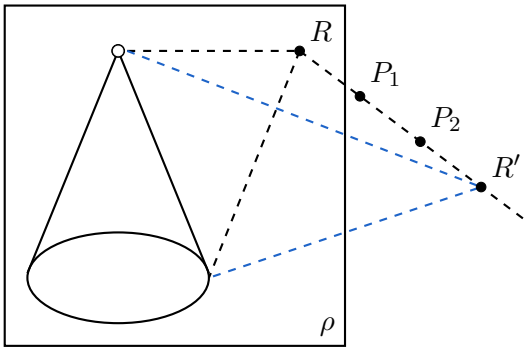
- Geval 1: $w(c') < d(\mathcal{C}_{n-3}(n-1,q)^\perp)$. Dan kan het codewoord c' niet bestaan, want $c' \in \mathcal{C}_{n-3}(n-1,q)^\perp$. Uit deze strijdigheid volgt dat de assumptie $\dim(\langle\mathcal{S}\rangle) \geq 4$ vals is. Bijgevolg behoort $\mathcal{S}$ tot een 3-dimensionale ruimte ρ. We kunnen dan $n-4$ keer projecteren naar deelruimten waar ρ in ligt en uiteindelijk naar ρ zelf. Deze projecties zullen het codewoord c niet veranderen en we vinden zo dankzij Stelling 3.3.6 dat $c \in \mathcal{C}_1(3,q)^\perp$. Omdat q even is, vormt $\mathcal{S}$ in dit geval dus een even verzameling van grootte $q(q+2)+2$ in $\mathrm{PG}(3,q)$.

- Geval 2: $w(c') = d(\mathcal{C}_{n-3}(n-1,q)^\perp) = w(c) - 2$. Dankzij Stelling 3.3.33 weten we dat $\mathrm{supp}(c')$ een hypercilinder in een 3-dimensionale ruimte ρ' is. Alle punten van $\mathcal{S}$ die geprojecteerd worden op de hypercilinder liggen in de 4-ruimte $\langle\rho', R\rangle = \rho$. Aangezien $w(c) = w(c') + 2$ liggen er hoogstens twee punten van $\mathcal{S}$ buiten ρ. Om te voldoen aan de stelling, moeten we enkel nog aantonen dat alle punten van $\mathcal{S}$ bevat zijn in ρ. Als er één punt $P_1 \in \mathcal{S}$ buiten ρ ligt, dan ook een tweede $P_2 \in \mathcal{S}$ op de rechte $\langle P_1, R\rangle$. Inderdaad, anders zou de projectie vanuit R geen hypercilinder meer zijn. Hierbij gebruiken we dat een rechte door R die een even aantal punten van $\mathcal{S}$ bevat projecteert op een punt met coëfficiënt nul, omdat q even is. Beschouw vervolgens een punt $R' \notin \mathcal{S}$ op de rechte $\langle P_1, P_2\rangle$ verschillend van R, zoals in Figuur 5.1. Omdat P_1 niet bevat is in ρ, is ook R' niet bevat in deze 4-ruimte. We kunnen dus projecteren vanuit R' naar een hypervlak door ρ. Als we dit doen verliezen we de bijdrage van de punten P_1 en P_2. Deze worden immers geprojecteerd op het punt R. Het punt R krijgt opnieuw coëfficiënt nul, omdat de rechte $\langle P_1, P_2\rangle$ een even aantal punten van $\mathcal{S}$ bevat. De overige punten van $\mathcal{S}$ blijven behouden, want deze zijn allemaal bevat in ρ. Het codewoord c'' dat we zo bekomen heeft dus gewicht $q(q+2)$ en $\mathrm{supp}(c'') = \mathcal{S} \setminus \{P_1, P_2\}$. Uit Stelling 3.3.33 volgt dat $\mathrm{supp}(c'')$ een hypercilinder $\mathcal{H}$ is. Dit betekent dat onze originele punten $\mathcal{S} \setminus \{P_1, P_2\}$ dezelfde hypercilinder $\mathcal{H}$ vormen. We kunnen dan het verschil nemen van het codewoord c'' dat geassocieerd is aan $\mathcal{H}$ en het codewoord c. Dit geeft een nieuw codewoord met gewicht $w(c) + w(c'') - 2w(c \cap c'') = 2$. Dit is echter kleiner dan het minimum gewicht van $\mathcal{C}_{n-2}(n,q)^\perp$. Het is dus onmogelijk dat de punten P_1 en P_2 niet in de 4-ruimte ρ liggen. We besluiten dat $\mathcal{S}$ volledig bevat is in de 4-dimensionale ruimte ρ. Merk ook op dat het niet uitmaakt naar welk hypervlak we projecteren vanuit R. Zolang dit hypervlak het punt R niet bevat, zullen we een hypercilinder vinden. We mogen dus spreken in de stelling van de projectie vanuit R zonder een hypervlak te specificeren. We zullen ook in verdere redeneringen als we spreken over een projectie vanuit een punt het hypervlak niet meer specificeren als dit niet nodig is.

- Geval 3: $w(c') = d(\mathcal{C}_{n-3}(n-1,q)^\perp)+1$. Hieruit volgt dat $w(c')$ oneven is, wat niet kan door Stelling 5.1.1. Zoals in het eerste geval volgt uit deze strijdigheid dat $\dim(\langle\mathcal{S}\rangle) \leq 3$. Hieruit vinden we dat $c \in \mathcal{C}_1(3,q)^\perp$. Of equivalent hiermee dat $\mathcal{S}$ een even verzameling van grootte $q(q+2)+2$ in $\mathrm{PG}(3,q)$ is. Hiermee hebben we het laatste geval en het bewijs afgerond.

■

Als we willen aantonen dat er geen codewoord bestaat van gewicht $q(q+2)+2$ in $\mathcal{C}_{n-2}(n,q)^\perp$, zijn er dus twee gevallen om te bekijken. In het eerste geval is het noodzakelijk dat we even verzamelingen van deze grootte uitsluiten in $\mathrm{PG}(3,q)$. Voor het tweede geval moeten we uitsluiten dat het mogelijk is om te projecteren en zo een hypercilinder in een 3-ruimte te vinden. Tijdens dit projecteren verliezen we juist twee punten. Dit feit zullen we later gebruiken om dit geval opnieuw op te splitsen in deelgevallen. Laten we eerst de even verzameling uitsluiten.



Figuur 5.1.: De hypercilinder die we vinden via projectie vanuit het punt $R \notin \mathrm{supp}(c)$ in de 4-ruimte ρ. De rechte $\langle R, R' \rangle$ ligt niet in ρ en bevat exact twee punten van $\mathrm{supp}(c)$, namelijk P_1 en P_2.

5.2. Geen even verzameling van grootte $q(q+2)+2$ in $\mathrm{PG}(3,q)$, met $q \in \{4,8\}$

In de literatuur is er al onderzoek verricht naar even verzamelingen in $\mathrm{PG}(3,4)$. In [30] wordt door Packer onder andere oneven verzamelingen besproken in $\mathrm{PG}(n,4)$. Aangezien een oneven verzameling het complement is van een even verzameling, volgt uit een classificatie van oneven verzamelingen een classificatie van even verzamelingen. Hieruit volgt dan ook hoe de code $\mathcal{C}_1(n,4)^\perp$ eruit ziet. In [30] kan zo de volledige gewichtsdistributie van de codes $\mathcal{C}_1(2,4)^\perp$, $\mathcal{C}_1(3,4)^\perp$ en $\mathcal{C}_1(4,4)^\perp$ worden beschreven. Merk op dat de karakterisering van oneven verzamelingen in $\mathrm{PG}(2,4)$ en $\mathrm{PG}(3,4)$ daar niet bewezen wordt. Packer vermeldt de resultaten van Tallini Scafati uit [42] en Hirschfeld en Hubaut uit [21]. Wij zullen in dit deel de resultaten en ideeën van Adriaensen uit [1] over de minimum even verzamelingen in $\mathrm{PG}(3,q)$, met $q = 4$ en 8, gebruiken en aanpassen. Zo kunnen we het bestaan van een even verzameling in $\mathrm{PG}(3,q)$ die grootte $q(q+2)+2$ heeft, met $q \in \{4,8\}$, uitsluiten. We doen dit in enkele stappen. Eerst beperken we het aantal punten van zo'n even verzameling die op een rechte kunnen liggen.

Stelling 5.2.1. *Als $\mathcal{S}$ een even verzameling in $\mathrm{PG}(3,q)$ is met grootte $q(q+2)+2$, met q even, dan bestaat er geen q-secant aan $\mathcal{S}$.*

Bewijs. Dit bewijs is geïnspireerd op de redenering van [1, Proposition 3.13], hier Stelling 3.3.30. Beschouw een even verzameling $\mathcal{S}$ in $\mathrm{PG}(3,q)$ zodat $|\mathcal{S}| = q(q+2)+2$. Veronderstel dat er een q-secant rechte l aan $\mathcal{S}$ bestaat. Noem T het unieke punt van $l \setminus \mathcal{S}$. Neem een willekeurig vlak π door l. Zoals eerder gezien in Stelling 3.3.26 is de verzameling $(\pi \cap \mathcal{S}) \triangle l$ een blokkerende verzameling in π. Aangezien zo'n verzameling minstens $q+1$ punten bevat, is $|(\mathcal{S} \cap \pi) \setminus l| \geq q$. Anderzijds zijn er door l juist $q+1$ verschillende vlakken en dus $q+1$ opties voor π. Hieruit volgt dat $|\mathcal{S}| \geq q + (q+1)q = q(q+2)$. We weten dat $|\mathcal{S}| = q(q+2)+2$. Dus is er exact één vlak π door l dat $q+2$ extra punten van $\mathcal{S}$ bevat. Hierbij gebruiken we dat $|\pi \cap \mathcal{S}|$ even moet zijn, waardoor we de twee extra punten niet over verschillende vlakken mogen spreiden. We vinden dus dat $|\pi \cap \mathcal{S}| = 2q+2$. Voor alle andere vlakken π' door l is $|\pi' \cap \mathcal{S}| = 2q$. In het bijzonder geldt er dat $|(\pi' \cap \mathcal{S}) \triangle l| = q+1$. Hieruit volgt zoals in het bewijs van Stelling 3.3.30 dat $\pi' \cap \mathcal{S}$ het symmetrisch verschil van twee rechten door T is. Eén van deze rechten is l. We noteren voor elk van de q vlakken π' de andere rechte als l_i, met $i \in \{1, \ldots, q\}$. Merk op dat we de rechte l in het begin mogen vervangen door elke rechte l_i. Dit betekent dat er geen vlak bestaat dat drie rechten bevat van de verzameling $\{l, l_1, \ldots, l_q\}$. We kunnen nu een hypercilinder $\mathcal{S}'$ maken die grotendeels

samenvalt met $\mathcal{S}$. Beschouw een willekeurig vlak π'' dat disjunct is aan het punt T. De snijpunten van de verzameling rechten $\{l, l_1, \ldots, l_q\}$ met π'' vormen een $(q+1)$-boog. Anders kunnen we een vlak maken door een rechte in π'' die minstens drie snijpunten bevat en het punt T. Dit vlak zou dan minstens drie rechten bevatten van de verzameling $\{l, l_1, \ldots, l_q\}$, wat een strijdigheid geeft. Dus vormen de snijpunten een $(q+1)$-boog in π''. Deze kunnen we op unieke wijze uitbreiden tot een hyperovaal $\mathcal{H}$ [20, Lemma 8.6]. Samen met het punt T kunnen we zo een hypercilinder $\mathcal{S}'$ definiëren. Het bijhorende codewoord c' heeft dan gewicht $q(q+2)$. We bekijken het codewoord $c - c'$, dan is

$$\begin{aligned} 0 < w(c-c') &= w(c) + w(c') - 2w(c \cap c') \\ &\leq q(q+2) + 2 + q(q+2) - 2q(q+1) \\ &\leq 2q^2 + 4q + 2 - 2q^2 - 2q \\ &\leq 2q + 2 < q^2 + 2q = q(q+2). \end{aligned}$$

Deze laatste ongelijkheid is waar omdat $2 < q^2$ voor $q = 8$. Het is echter onmogelijk om een niet-nul codewoord te hebben met gewicht kleiner dan $q(q+2)$, dus vinden we de gezochte strijdigheid. ■

Met behulp van deze stelling kunnen we onmiddellijk het bestaan van even verzamelingen met grootte $q(q+2)+2$ in $\mathrm{PG}(3,4)$ uitsluiten. Zoals hierboven besproken is dit een gekend resultaat. Voor de volledigheid voegen we dit kort alternatief bewijs toe.

Stelling 5.2.2. *Er bestaat geen even verzameling $\mathcal{S}$ met grootte 26 in $\mathrm{PG}(3,4)$.*

Bewijs. Uit de vorige stelling weten we dat er geen 4-secanten bestaan aan een even verzameling $\mathcal{S}$ in $\mathrm{PG}(3,4)$ met grootte 26. Er bestaan dus enkel 0- en 2-secanten. Neem een 2-secant rechte l aan $\mathcal{S}$. Noem P een van de punten van $l \cap \mathcal{S}$. Elke rechte door P is dan een 2-secant. Bijgevolg bevat elk vlak door l juist q andere punten van $\mathcal{S}$. Aangezien er $q+1 = 5$ vlakken door l zijn, vinden we dat $|\mathcal{S}| = 2 + 5 \cdot 4 = 22$. Echter het gegeven zegt dat $|\mathcal{S}| = 26$, dus we vinden een strijdigheid. We besluiten dat er zo geen even verzameling bestaat. ■

Bewijzen dat er geen even verzameling $\mathcal{S}$ van grootte $q(q+2)+2 = 82$ bestaat in $\mathrm{PG}(3,8)$ zal wat meer werk vragen. We sluiten hiervoor eerst het bestaan van 6-secant rechten aan $\mathcal{S}$ uit. Nadien tonen we aan dat elk punt van $\mathcal{S}$ op juist vier verschillende 4-secant rechten ligt.

Stelling 5.2.3. *Er bestaat geen even verzameling $\mathcal{S}$ in $\mathrm{PG}(3,8)$ met grootte 82 zodat die een 6-secant aan $\mathcal{S}$ bevat.*

Bewijs. Dit bewijs is een aanpassing van een redenering uit [1], hier bespreken we deze in Stelling 3.3.31. Beschouw een even verzameling $\mathcal{S}$ in $\mathrm{PG}(3,8)$ met grootte 82. Veronderstel dat l een 6-secant rechte aan $\mathcal{S}$ is. We tonen eerst aan dat er een Rédei vlak π door l bestaat, i.e. $|(\mathcal{S} \cap \pi) \setminus l| = q$. Veronderstel dat dit niet waar is, dan bevat elk vlak π door l minstens $q+2$ extra punten van $\mathcal{S}$. Aangezien er $q+1$ vlakken zijn door elke rechte, vinden we:

$$|\mathcal{S}| = 82 \geq 6 + (q+1)(q+2) = 96.$$

Dit kan niet, dus bestaat er een Rédei vlak π door l. We bekijken vervolgens de blokkerende verzameling $(\pi \cap \mathcal{S}) \triangle l$ in het vlak π. Deze heeft grootte $|(\mathcal{S} \cap \pi) \setminus l| + |l \setminus \mathcal{S}| = q + 3 = 11$. Er bestaat geen 8-secant aan $\mathcal{S}$ dankzij Stelling 5.2.1. Hierdoor bevat de blokkerende verzameling $(\pi \cap \mathcal{S}) \triangle l$ geen rechten. Uit het resultaat van Bruen in [12], dat we eerder ook gebruikten, weten we dat zo'n blokkerende verzameling minstens 13 punten bevat in $\mathrm{PG}(2,8)$. Dit geeft de verwachte strijdigheid. ■

Gevolg 5.2.4. *Er bestaan enkel 0-, 2- en 4-secant rechten aan een even verzameling met grootte 82 in* $\mathrm{PG}(3,8)$.

Bewijs. Dit volgt rechtstreeks uit de definitie van een even verzameling en Stellingen 5.2.1 en 5.2.3. ∎

Lemma 5.2.5. *Gegeven een even verzameling* $\mathcal{S}$ *in* $\mathrm{PG}(3,8)$*, met* $|\mathcal{S}| = 82$*, dan zijn er door elk punt* $P \in \mathcal{S}$ *juist vier verschillende 4-secanten.*

Bewijs. Beschouw een even verzameling $\mathcal{S}$ in $\mathrm{PG}(3,8)$ zodat $|\mathcal{S}| = 82$. Door een punt $P \in \mathcal{S}$ zijn er enkel 2- of 4-secant rechten dankzij Gevolg 5.2.4. We noteren het aantal 4-secanten door P met x. Er zijn dan $\theta_2 - x = 73 - x$ verschillende 2-secanten door P. We bepalen wat x is door het aantal punten van $\mathcal{S}$ te tellen via de rechten door P. Dit geeft:

$$82 = |\mathcal{S}| = 1 + 3x + (73 - x) = 74 + 2x \Rightarrow x = 4.$$

∎

We kunnen via dit lemma de mogelijke combinaties van het aantal 18- en 16-secant vlakken aan $\mathcal{S}$ bepalen. Dit zullen we doen in de volgende stelling. In Stelling 5.2.7 daarna bewijzen we via verdere tellingen dat geen enkel van deze combinaties zich kan voordoen. Het idee om te kijken naar de ligging van de 4-secant rechten door een punt komt uit [1, Proposition 3.16]. Ook het idee voor de eerste dubbele telling uit het bewijs van Stelling 5.2.7 en om daar te kijken naar de gevolgen van de aanwezigheid van de factor 7 komt uit [1, Proposition 3.16]. Wij hebben deze propositie besproken en dit is hier Stelling 3.3.32. Omdat we hier echter twee extra punten hebben, zijn er andere mogelijkheden voor de verdeling van de punten van $\mathcal{S}$ over de vlakken. Het uitsluiten van deze gebeurt hier dan ook op een verschillende manier.

Stelling 5.2.6. *Gegeven een even verzameling* $\mathcal{S}$ *in* $\mathrm{PG}(3,8)$*, met* $|\mathcal{S}| = 82$*. We kunnen de punten van* $\mathcal{S}$ *opsplitsen in drie verzamelingen* $\mathcal{V}_1$*,* $\mathcal{V}_2$ *en* $\mathcal{V}_3$ *op basis van hoeveel vlakken door een punt een 18- of 16-secant vlak zijn. Voor elk punt* $P \in \mathcal{V}_i$*, met* $i \in \{1,2,3\}$*, weten we hoeveel vlakken door* P *een* x*-secant vlak zijn,* $x \in \{18,16,14,12,10\}$*. Dit is beschreven in Tabel 5.1.*

Bewijs. Stel dat $\mathcal{S}$ een even verzameling is in $\mathrm{PG}(3,8)$ met $|\mathcal{S}| = 82$. Neem een punt $P \in \mathcal{S}$. Uit het vorige lemma weten we dat er vier verschillende 4-secant rechten zijn door P. We gebruiken de ligging van deze rechten om P toe te wijzen aan $\mathcal{V}_1$, $\mathcal{V}_2$ of $\mathcal{V}_3$.

- Als de vier 4-secant rechten door P in één vlak π liggen, dan wijzen we P toe aan de verzameling $\mathcal{V}_1$. Het vlak π bevat naast deze vier rechten nog vijf andere rechten door P. Dit zijn door Gevolg 5.2.4 dan 2-secant rechten. We vinden dus dat $|\mathcal{S} \cap \pi| = 1 + 3 \cdot 4 + 1 \cdot 5 = 18$. Er volgt ook uit Gevolg 5.2.4 dat als een punt van $\mathcal{S}$ in een 18-secant vlak ligt, dan moeten er vier verschillende 4-secant rechten door dit punt in het vlak liggen. Analoog kan men aantonen dat als er respectievelijk drie, twee, één of nul verschillende 4-secant rechten door een punt van $\mathcal{S}$ in een vlak liggen als en slechts als dit vlak een 16-, 14-, 12- of 10- secant vlak is. Deze redenering zullen we gedurende het hele bewijs in onze gedachten houden om de vlakken te tellen. Omdat er maar vier verschillende 4-secant rechten zijn door het punt P, ligt P op hoogstens één 18-secant vlak. De verzameling $\mathcal{V}_1$ bestaat dus uit de punten van $\mathcal{S}$ die op exact één 18-secant vlak liggen. Alle andere vlakken door P bevatten hoogstens één 4-secant rechte door P. In het bijzonder ligt P in geen enkel 16- of 14-secant vlak. Veronderstel dat l een 4-secant rechte is door P. De vlakken door l verschillend van het 18-secant vlak π zijn bijgevolg 12-secant vlakken. Door een rechte zijn er in totaal negen vlakken, dus de 4-secant l ligt nog in acht verschillende 12-secant vlakken. Zo vinden we dat P in $4 \cdot 8 = 32$

verschillende 12-secant vlakken ligt. In $\mathrm{PG}(3,8)$ zijn er door een punt $\begin{bmatrix}3\\2\end{bmatrix}_8 = 73$ vlakken. Alle vlakken door P die we nog niet hebben geteld, moeten 10-secant vlakken zijn. Bijgevolg zijn er door P juist $73 - 1 - 32 = 40$ verschillende 10-secant vlakken.

- Als er juist drie van de vier verschillende 4-secant rechten door P in een vlak π liggen, dan zeggen we dat $P \in \mathcal{V}_2$. De verzameling $\mathcal{V}_2$ bestaat dus uit punten P zodat P in één 16-secant vlak en nul 18-secant vlakken ligt. De 4-secant rechte door P die niet in π ligt, noemen we l. De andere 4-secant rechten door P duiden we aan met m_1, m_2 en m_3. De rechte l vormt met m_i, met $i \in \{1,2,3\}$, een 14-secant vlak door P. Zo zien we dat P in drie verschillende 14-secant vlakken ligt. Het punt P ligt voor de rest enkel nog op 12- en 10-secant vlakken. We tellen eerst de 12-secant vlakken. Deze bevatten allemaal juist één 4-secant rechte door P. We hadden door de rechte l al drie 14-secant vlakken gevonden. De zes andere vlakken door l zijn noodzakelijk 12-secant vlakken. Om het totale aantal 12-secant vlakken door P te tellen, bepalen we ook hoeveel vlakken van die soort er zijn door de rechten m_i. We weten dat er door elke m_i één 16-secant vlak π en één 14-secant vlak $\langle m_i, l\rangle$ is. De zeven andere vlakken door m_i, zijn dan 12-secant vlakken. We vinden dus dat er door P in totaal $6 + 3 \cdot 7 = 27$ verschillende 12-secant vlakken zijn. Alle vlakken door P die we nog niet besproken hebben, zijn 10-secant vlakken. Dit zijn er $73 - 1 - 3 - 27 = 42$.
- Er blijft nog één mogelijkheid over: er liggen hoogstens twee 4-secant rechten door P in elk vlak. Deze punten vormen de derde verzameling $\mathcal{V}_3$. Ze kunnen niet in een 18-secant vlak of een 16-secant vlak liggen. We bepalen het aantal 14-secant vlakken waartoe P behoort. Deze worden bepaald door twee verschillende 4-secant rechten door P. Voor de eerste rechte hebben we vier keuzes, voor de tweede rechte dan nog maar drie keuzes. We vinden dus dat P in $\frac{4\cdot 3}{2} = 6$ verschillende 14-secant vlakken ligt. We bepalen het aantal 12-secant vlakken waarin P ligt zoals in de vorige puntjes. Elke 4-secant l door P ligt in drie 14-secant vlakken zoals we eerder opmerkten. De zes overige vlakken door l zijn dus 12-secant vlakken. Bijgevolg ligt P in $4 \cdot 6 = 24$ verschillende 12-secant vlakken. We besluiten dat P daarnaast in $73 - 6 - 24 = 43$ verschillende 10-secant vlakken ligt.

Hiermee hebben we aangetoond wat we wilden bewijzen. ■

	$P \in \mathcal{V}_1$	$P \in \mathcal{V}_2$	$P \in \mathcal{V}_3$
18-secant vlak	1	0	0
16-secant vlak	0	1	0
14-secant vlak	0	3	6
12-secant vlak	32	27	24
10-secant vlak	40	42	43

Tabel 5.1.: Elk punt $P \in \mathcal{S}$ behoort tot één van de drie verzamelingen $\mathcal{V}_1$, $\mathcal{V}_2$ en $\mathcal{V}_3$. Afhankelijk hiervan geven we weer hoe de vlakken door P eruit zien.

Stelling 5.2.7. *Er bestaat geen even verzameling $\mathcal{S}$ in $\mathrm{PG}(3,8)$ zodat $|\mathcal{S}| = 82$.*

Bewijs. Zij $\mathcal{S}$ een even verzameling in $\mathrm{PG}(3,8)$ met grootte 82. Veronderstel dat de verzamelingen $\mathcal{V}_1$, $\mathcal{V}_2$ en $\mathcal{V}_3$ gedefinieerd zijn zoals in de vorige stelling. We noteren het aantal i-secant vlakken als m_i. Elk punt in $\mathcal{V}_1$ ligt in juist één 18-secant vlak en elk zo'n vlak bevat 18 punten van $\mathcal{V}_1$. Dus is $|\mathcal{V}_1| = 18m_{18}$. Analoog is $|\mathcal{V}_2| = 16m_{16}$. Alle overige punten van $\mathcal{S}$ behoren tot $\mathcal{V}_3$, derhalve is $|\mathcal{V}_3| = 82 - 18m_{18} - 16m_{16}$. We zouden graag bepalen wat de mogelijke groottes zijn van deze verzamelingen. Hiervoor voeren we een dubbele telling uit van de koppels (P,π) met P een punt

en π een 14-secant vlak zodat $P \in (\pi \cap \mathcal{S})$. Langs de ene kant zijn er m_{14} verschillende 14-secant vlakken die elk 14 punten bijdragen aan de telling. Dus zijn er $14m_{14}$ koppels. Langs de andere kant kunnen we deze koppels ook tellen via de punten. De punten uit $\mathcal{V}_1$ liggen niet op een 14-secant vlak en leveren dus geen bijdrage. Een punt van $\mathcal{V}_2$ ligt in drie zo'n vlakken. De bijdrage van de verzameling $\mathcal{V}_2$ aan het aantal koppels is dan ook $3 \cdot 16m_{16}$. Een punt van het derde type ligt in zes verschillende 14-secant vlakken en er zijn zo $82 - 18m_{18} - 16m_{16}$ punten. Dit geeft een bijdrage van $6(82 - 18m_{18} - 16m_{16})$. Wanneer we deze twee tellingen vergelijken, vinden we:

$$\begin{aligned} 14m_{14} &= 3 \cdot 16m_{16} + 6(82 - 18m_{18} - 16m_{16}) \\ &= 12(4m_{16} + 41 - 9m_{18} - 8m_{16}) \\ &= 12(41 - 9m_{18} - 4m_{16}). \end{aligned}$$

Aangezien het linkerlid een factor 7 bevat, moet deze ook aanwezig zijn in het rechterlid. Omdat 12 en 7 copriem zijn, komt dit neer op $41 - 9m_{18} - 4m_{16} = 0 \pmod 7$. Aangezien we bij onze tellingen werken met natuurlijke getallen is m_{18} hoogstens 4. We bepalen voor alle mogelijke waarden van m_{18} wat m_{16} kan zijn. We zullen telkens een waarde voor m_{16} vinden modulo 7. Nadien controleren we welke bijhorende natuurlijke getallen een niet negatieve waarde geven voor $41 - 9m_{18} - 4m_{16}$. De eerste keer zullen we deze controle expliciet doen, daarna geven we onmiddellijk het resultaat.

- Als $m_{18} = 0$:

$$\begin{aligned} & 41 = 4m_{16} \pmod 7 \\ \iff & 82 = m_{16} \pmod 7 \\ \iff & 5 = m_{16} \pmod 7. \end{aligned}$$

  De waarde $m_{16} = 5$ is een optie, want $41 - 9 \cdot 0 - 4 \cdot 5 = 21$. Maar de volgende waarde $m_{16} = 5 + 7 = 12$ niet mogelijk. We vinden dan immers $41 - 9 \cdot 0 - 4 \cdot 12 = -7$.

- Als $m_{18} = 1$:

$$\begin{aligned} & 41 - 9 = 4m_{16} \pmod 7 \\ \iff & 64 = m_{16} \pmod 7 \\ \iff & 1 = m_{16} \pmod 7. \end{aligned}$$

  Hieruit volgt dat $m_{16} = 1$ of $m_{16} = 8$. Deze laatste mogelijkheid geeft $m_{14} = 0$.

- Als $m_{18} = 2$:

$$\begin{aligned} & 41 - 18 = 4m_{16} \pmod 7 \\ \iff & 46 = m_{16} \pmod 7 \\ \iff & 4 = m_{16} \pmod 7. \end{aligned}$$

  Dit geeft $m_{16} = 4$.

- Als $m_{18} = 3$:

$$\begin{aligned} & 41 - 27 = 4m_{16} \pmod 7 \\ \iff & 28 = m_{16} \pmod 7 \\ \iff & 0 = m_{16} \pmod 7. \end{aligned}$$

Hieruit volgt $m_{16} = 0$.

- Als $m_{18} = 4$:

$$\begin{aligned} & 41 - 36 = 4m_{16} \pmod 7 \\ \iff & 10 = m_{16} \pmod 7 \\ \iff & 3 = m_{16} \pmod 7. \end{aligned}$$

We besluiten dat dit geval niet kan, want $41 - 9 \cdot 4 - 4 \cdot 3 = -7$.

Wanneer we deze waarden substitueren in bovenstaande formules voor m_{14}, $|\mathcal{V}_1|$, $|\mathcal{V}_2|$ en $|\mathcal{V}_3|$ bekomen we Tabel 5.2.

	m_{18}	m_{16}	m_{14}	$\lvert\mathcal{V}_1\rvert$	$\lvert\mathcal{V}_2\rvert$	$\lvert\mathcal{V}_3\rvert$
Geval 1	0	5	18	0	80	2
Geval 2	1	1	24	18	16	48
Geval 3	1	8	0	18	128	-64
Geval 4	2	4	6	36	64	-18
Geval 5	3	0	12	54	0	28

Tabel 5.2.: De mogelijkheden voor de groottes van $\mathcal{V}_1$, $\mathcal{V}_2$, $\mathcal{V}_3$, m_{18}, m_{16} en m_{14}.

We zien onmiddellijk dat geval 3 en 4 niet mogelijk zijn. We bewijzen nu dat de overige gevallen ook niet kunnen voorkomen. Hierbij zullen we telkens uitkomen dat het aantal 10-secant vlakken geen natuurlijk getal kan zijn.

Veronderstel dat we ons in het eerste geval bevinden. We kunnen het aantal 10-secant vlakken tellen via Tabellen 5.2 en 5.1. Er zijn 80 punten in de verzameling $\mathcal{V}_2$. Deze liggen elk op 42 verschillende 10-secant vlakken. Daarnaast zijn er nog 2 punten in $\mathcal{V}_3$, die elk tot 43 verschillende 10-secant vlakken behoren. Als we al deze aantallen optellen en delen door 10, want we hebben elk 10-secant vlak 10 keer geteld, vinden we het aantal 10-secant vlakken. Dit geeft $\frac{42 \cdot 80 + 43 \cdot 2}{10} = 344,6$, wat dus een strijdigheid is.

We gaan er vervolgens vanuit dat we ons in geval 2 bevinden. We tellen opnieuw het aantal 10-secant vlakken via Tabel 5.1. Er zijn 18 punten in $\mathcal{V}_1$ die elk in 40 verschillende 10-secant vlakken liggen. De 16 punten van $\mathcal{V}_2$ behoren elk tot 42 zo'n vlakken en de 48 punten van $\mathcal{V}_3$ liggen elk in 43 verschillende 10-secant vlakken. We bekomen zo $\frac{18 \cdot 40 + 16 \cdot 42 + 48 \cdot 43}{10} = 345,6$ verschillende 10-secant vlakken. Dit kan natuurlijk niet.

Stel nu dat het laatste geval waar is. Wanneer we opnieuw op dezelfde manier het aantal 10-secant vlakken tellen, bekomen we $\frac{54 \cdot 40 + 28 \cdot 43}{10} = 336,4$ verschillende 10-secant vlakken. Hiermee is het laatste geval uitgesloten. Er bestaan dus geen even verzamelingen van grootte 82 in $\mathrm{PG}(3, 8)$. ■

Zo hebben we al de eerste mogelijkheid van Stelling 5.1.7 geëlimineerd. We vatten in onderstaand gevolg samen wat de resterende situatie is. In het volgende deel is het doel om aan te tonen dat ook dit niet mogelijk is.

Gevolg 5.2.8. *Beschouw een codewoord $c \in \mathcal{C}_{n-2}(n,q)^\perp$, met $q \in \{4, 8\}$. Als $w(c) = q(q+2)+2$, dan is $\dim(\langle \mathrm{supp}(c) \rangle) = 4$ en bestaat er een punt $R \notin \mathrm{supp}(c)$ in de 4-ruimte $\langle \mathrm{supp}(c) \rangle$ zodat de projectie van c uit R een hypercilinder in een 3-ruimte is.*

Bewijs. Stel dat $c \in \mathcal{C}_{n-2}(n,q)^\perp$, met $q \in \{4,8\}$ en $w(c) = q(q+2)+2$. Uit Stellingen 5.2.2 en 5.2.7 volgt dat het codewoord c niet bestaat als $n = 3$, want dan is dit equivalent met het bestaan van een even verzameling met grootte $q(q+2)+2$. Dus moet de support van c minstens een 4-ruimte opspannen. Uit Stelling 5.1.7 volgt dan het te bewijzen. ∎

5.3. Geen codewoord met gewicht $q(q+2)+2$ in $\mathcal{C}_{n-2}(n,8)^\perp$

Veronderstel dat c een codewoord is met gewicht $q(q+2)+2$ van de code $\mathcal{C}_{n-2}(n,q)^\perp$, met $q = 8$. Uit Gevolg 5.2.8 volgt dat $\mathrm{supp}(c)$ een 4-ruimte opspant. Door meerdere keren te projecteren indien nodig, vinden we dat $c \in \mathcal{C}_2(4,q)^\perp$. Het is dus voldoende om $n = 4$ te bestuderen. We zullen gebruiken dat $\mathrm{supp}(c)$ niet te veel punten mag gemeen hebben met een hypercilinder $\mathcal{H}$. Want als we het verschil bekijken van c en het codewoord geassocieerd aan $\mathcal{H}$ vinden we dan een te klein codewoord. Hieruit zal volgen dat het punt R uit Gevolg 5.2.8 op een 3-secant ligt. Tenslotte zullen we bewijzen dat ook dit een strijdigheid geeft. We bouwen deze redenering op in verschillende stappen. In sommige stappen zal $q = 4$ te klein zijn. Vandaar dat we ons op een bepaald moment zullen beperken tot $q = 8$. Laten we beginnen met onderstaand lemma te bewijzen dat geldig is voor $q = 4$ en 8.

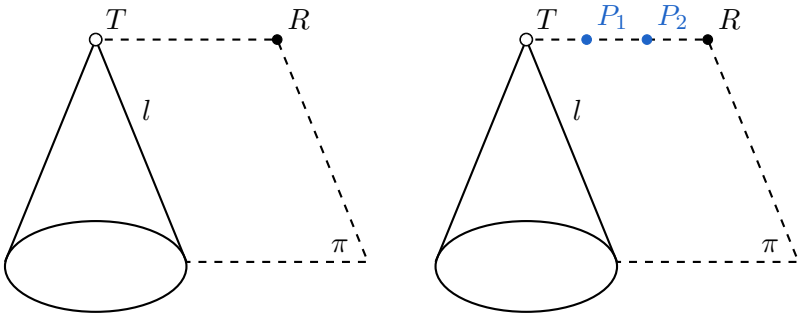
Lemma 5.3.1. *Beschouw een codewoord $c \in \mathcal{C}_2(4,q)^\perp$, met $q \in \{4,8\}$, zodat $w(c) = q(q+2)+2$. Veronderstel dat een punt $R \notin \mathcal{S}$ op minstens één raaklijn aan $\mathcal{S}$ ligt. Het punt R ligt dan op juist één 2- of 3-secant rechte aan $\mathrm{supp}(c)$, en alle andere rechten door R zijn 0- en 1-secant rechten.*

Bewijs. Beschouw het codewoord c en het punt R zoals in het gegeven. Neem een willekeurig hypervlak π dat het punt R niet bevat. Wanneer we c projecteren vanuit R op π vinden we een codewoord $c' \in \mathcal{C}_1(3,q)^\perp$. Omdat R op een raaklijn ligt, is c' niet de nulvector. Ook is $\mathrm{supp}(c')$ een even verzameling. Uit Stellingen 5.2.2 en 5.2.7 weten we dat er geen even verzamelingen in $\mathrm{PG}(3,q)$ bestaan met grootte $q(q+2)+2$. Dus is $|\mathrm{supp}(c')| = q(q+2)$. Er volgt uit Stelling 3.3.33 dat de punten van $\mathrm{supp}(c')$ een hypercilinder vormen. Dit betekent dat exact twee punten van $\mathrm{supp}(c)$ bij het projecteren geen bijdrage leveren aan $\mathrm{supp}(c')$. Dus bevat een rechte door R hoogstens drie punten van $\mathrm{supp}(c)$, want anders verliezen we te veel punten bij de projectie. Merk op dat een 2-secant rechte door R projecteert op een punt met coëfficiënt nul omdat q even is. Dus zijn er juist twee mogelijkheden om twee punten te verliezen. Ofwel ligt het punt R op één 3-secant rechte, deze drie punten projecteren dan op één punt met coëfficiënt 1. Als dit niet het geval is, moet R op één 2-secant rechte liggen. In beide gevallen zijn alle andere rechten door P een 0- of 1-secant rechte, opdat de projectie een hypercilinder is. ∎

Het is duidelijk dat het punt R uit Gevolg 5.2.8 voldoet aan de voorwaarden van Lemma 5.3.1. We vinden zo twee gevallen: R ligt op een 2-secant of R ligt op een 3-secant. In het geval van de 2-secant, splitsen we dit op in de twee deelgevallen. Namelijk de top T van de hypercilinder $\mathcal{H}$, die we vinden na projectie, ligt ofwel op de 2-secant ofwel niet. Zo vinden we dus drie mogelijke scenario's. Afhankelijk hiervan bevatten de vlakken door een q-secant l van $\mathcal{H}$ en het punt R meer of minder punten van $\mathrm{supp}(c)$. We bekijken enkele mogelijke vormen van zo'n vlak $\langle l, R\rangle$ in de onderstaande lemma's. Dit is de eerste stap om de punten van $\mathrm{supp}(c)$ in de vorm van een hypercilinder te krijgen als R op een 2-secant zou liggen.

Lemma 5.3.2. *Gegeven een codewoord $c \in \mathcal{C}_2(4,q)^\perp$, $q = 8$, met $w(c) = q(q+2)+2$ en een punt $R \notin \mathrm{supp}(c)$ zodat de projectie van c uit R een hypercilinder is in een 3-ruimte. Stel dat l een q-secant rechte is van deze hypercilinder. Als het vlak $\langle l, R\rangle$ precies q punten van $\mathrm{supp}(c)$ bevat, dan vormen deze punten een q-secant.*

Bewijs. Beschouw een codewoord $c \in \mathcal{C}_2(4,q)^\perp$, een punt R en de rechte l zoals in het gegeven. We noteren de support van c als $\mathcal{S}$. Veronderstel dat π een vlak door R en de rechte l is zodat $|\pi \cap \mathcal{S}| = q$. In de linkse tekening van Figuur 5.2 geven we dit grafisch weer. De top van de hypercilinder noemen we T. We weten uit Lemma 5.3.1 dat R op precies één 2-secant of één 3-secant ligt. Deze kan niet in π liggen, omdat $|\pi \cap \mathcal{S}| = q$ en de projectie vanuit R in π de q-secant l geeft. Alle rechten door R in π zijn dus 0- of 1-secanten. De punten van l, verschillend van het punt T, noemen we Q_i, met $i \in \{1, \ldots, q\}$. De rechte $\langle T, R\rangle$ bevat geen punten van $\mathcal{S}$, want T behoort niet tot de hypercilinder. De rechten $\langle Q_i, R\rangle$ bevatten elk juist één punt van $\mathcal{S}$, want Q_i behoort wel tot de hypercilinder. Hieruit volgt dat elk punt R' in $\pi \setminus \langle T, R\rangle$, met $R' \notin \mathcal{S}$ op minstens één raaklijn ligt. We weten immers al dat R' op één van de rechten $\langle Q_i, R\rangle$ ligt. Uit Lemma 5.3.1 volgt daarnaast dat R' op hoogstens één 2- of 3-secant m aan $\mathcal{S}$ ligt. Dit betekent dat er door R' in het vlak π minstens $q-3$ raaklijnen zijn. Als de rechte m in het vlak π ligt, vinden we na projectie door R' een rechte m' die $q-2$ punten van het nieuwe codewoord bevat. Maar het nieuwe codewoord moet een hypercilinder zijn. Dus de rechte m' kan niet bestaan. Hierdoor ligt de rechte m niet in het vlak π. In het bijzonder ligt elk punt $R' \in \pi \setminus \langle T, R\rangle$, met $R' \notin \mathcal{S}$, enkel op 0- en 1-secanten aan $\mathcal{S}$ in π. Neem dan twee verschillende punten $P_1, P_2 \in \mathcal{S} \cap \pi$. Beschouw een punt P op de rechte $\langle P_1, P_2\rangle$ verschillend van het snijpunt $\langle P_1, P_2\rangle \cap \langle T, R\rangle$. Als het punt P niet in $\mathcal{S}$ ligt, is het een punt van de vorm R'. Maar het ligt ook op de secant $\langle P_1, P_2\rangle$ in π, wat niet kan. Dus zijn alle punten van de rechte $\langle P_1, P_2\rangle$, behalve het punt $\langle P_1, P_2\rangle \cap \langle T, R\rangle$, bevat in $\mathcal{S}$. Aangezien $|\pi \cap \mathcal{S}| = q$ hebben we bewezen dat alle punten van $\mathcal{S}$ in π een q-secant vormen. ■



Figuur 5.2.: In beide figuren zien we de hypercilinder met top T die we vinden via projectie vanuit het punt R in $\mathrm{PG}(4,q)$. In stippellijnen duiden we het vlak $\pi = \langle R, l\rangle$ aan, hierin is l na de projectie een q-secant van de hypercilinder. Links gaan we er vanuit dat het vlak π precies q punten van $\mathcal{S}$ bevat. Rechts bevat dit vlak $q+2$ punten van $\mathcal{S}$ en meer specifiek bevat de rechte $\langle T, R\rangle$ twee punten van $\mathcal{S}$: P_1 en P_2.

Lemma 5.3.3. *Gegeven een codewoord $c \in \mathcal{C}_2(4,q)^\perp$, $q = 8$, met $w(c) = q(q+2)+2$ en een punt $R \notin \mathrm{supp}(c)$ zodat de projectie van c uit R een hypercilinder $\mathcal{H}$ is in een 3-ruimte. Stel dat l een q-secant rechte is van deze hypercilinder. Als het vlak $\pi = \langle l, R\rangle$ precies $q+2$ punten van $\mathrm{supp}(c)$ bevat en er ligt een 2-secant rechte door R in π, dan bestaat er een $(q+1)$-secant die R niet bevat aan $\mathrm{supp}(c)$ in π.*

Bewijs. Veronderstel dat $c \in \mathcal{C}_2(4,q)^\perp$ een codewoord is met gewicht $q(q+2)+2$. Stel dat het punt R en de rechte l zijn zoals in het gegeven. Veronderstel dat het vlak $\pi = \langle R, l\rangle$ de enige 2-secant door R bevat. We gaan er ook vanuit dat π juist $q+2$ punten van $\mathcal{S}$, de support van c, bevat. De rechten door R verschillend van de 2-secant in π zijn door Lemma 5.3.1 raaklijnen. Omdat $l \subset \pi$ een q-secant is van de hypercilinder $\mathcal{H}$, projecteert R de punten van de 2-secant op de top T van $\mathcal{H}$. We visualiseren dit in de rechtse tekening van Figuur 5.2. De twee punten van $\mathcal{S}$ op de rechte $\langle T, R\rangle$ noemen we P_1 en P_2. Veronderstel dat de q punten van de verzameling $(\pi \cap \mathcal{S}) \setminus \{P_1, P_2\}$

niet collineair zijn. We bewijzen dat dit niet kan. We bepalen eerst een ondergrens voor het aantal secanten door een punt P van $(\pi \cap \mathcal{S}) \setminus \{P_1, P_2\}$ in π. Neem een willekeurige secant m door P, merk op dat $R \notin m$. Er ligt een punt $R' \notin \mathcal{S}$ op m, want anders zou de verzameling $(\pi \cap \mathcal{S}) \setminus \{P_1, P_2\}$ collineair zijn. Dit punt R' ligt ook op de raaklijn $\langle R, R' \rangle$. Uit Lemma 5.3.1 toegepast op R' volgt dat de rechte m een 2- of 3-secant is. Dus bevat elke rechte door P hoogstens twee extra punten van $\mathcal{S}$. Er zijn $q+1$ punten van $\mathcal{S}$ in π om te verdelen over de rechten door P. Uit het duivenhokprincipe volgt er dat het punt P op minstens $\frac{q}{2}+1$ secanten ligt. Zo hebben we onze beloofde ondergrens gevonden. Neem punten P_3 en $P_4 \in (\pi \cap \mathcal{S}) \setminus \{P_1, P_2\}$ zodat P_4 niet op de rechte $\langle P_1, P_3 \rangle$ ligt. Het is steeds mogelijk om zo'n punt P_4 te kiezen omdat $\langle P_1, P_3 \rangle$ een 2- of 3-secant is. Dus sluiten we voor de keuze van P_4 hoogstens 4 punten van $\mathcal{S}$ uit. Aangezien $|\mathcal{S} \cap \pi| = q+2$ volgt er dat we steeds een punt P_4 kunnen kiezen. Door het punt P_4 zijn er minstens $\frac{q}{2}+1$ secanten. Aangezien $\frac{q}{2}+1 > 3$, snijdt minstens één secant hiervan de rechte $\langle P_1, P_3 \rangle$ in een punt $R' \notin \mathcal{S}$. Dit punt R' ligt dan op de raaklijn $\langle R, R' \rangle$ en twee secanten $\langle P_1, P_3 \rangle$ en $\langle R', P_4 \rangle$. Dit geeft een strijdigheid met Lemma 5.3.1. Onze assumptie dat de punten in $(\pi \cap \mathcal{S}) \setminus \{P_1, P_2\}$ niet collineair zijn, is dus vals. Afhankelijk van hun snijpunt met de rechte $\langle P_1, P_2 \rangle$ vormen ze een q- of $(q+1)$-secant rechte. We noemen deze rechte vanaf nu m.

We tonen vervolgens aan dat m de rechte $\langle P_1, P_2 \rangle$ snijdt in P_1 of P_2. Dit betekent dat m een $(q+1)$-secant is. Stel dat m toch een q-secant is. Neem een punt R' in het vlak π dat niet op één van de rechten $\langle P_1, P_2 \rangle$ of m ligt. Merk op dat dan $R' \notin \mathcal{S}$, want alle punten van $\mathcal{S}$ liggen op de rechten $\langle P_1, P_2 \rangle$ en m. Daarnaast is het punt $m \cap \langle P_1, P_2 \rangle$ het enige punt van de rechte m dat niet tot $\mathcal{S}$ behoort. Omdat $R' \notin \langle P_1, P_2 \rangle$ snijdt de rechte $\langle R', P_1 \rangle$ de rechte m in een punt van $\mathcal{S}$. Hieruit volgt dat de rechte $\langle R', P_1 \rangle$ een secant is. Analoog is de rechte $\langle R', P_2 \rangle$ een secant. Maar dan ligt het punt R' op te veel secanten en vinden we een strijdigheid met Lemma 5.3.1. We besluiten dat m een $(q+1)$-secant is. ■

Als R op een 2-secant ligt, volgt uit bovenstaande lemma's dat er q- of $(q+1)$-secanten bestaan aan $\mathrm{supp}(c)$. Merk op dat deze telkens de rechte $\langle T, R \rangle$ snijden. De volgende stap is om zoveel mogelijk van deze secanten door hetzelfde punt van de rechte $\langle T, R \rangle$ te laten gaan. Dit doen we in onderstaand lemma en stelling. Afhankelijk van de ligging van de 2-secant door R, zullen we Lemma 5.3.4 of Stelling 5.3.5 kunnen toepassen.

Lemma 5.3.4. *Gegeven een codewoord $c \in \mathcal{C}_2(4,q)^\perp$, $q = 8$, zodat $w(c) = q(q+2)+2$. Veronderstel dat $\langle T, R \rangle$ een rechte is die geen punten van $\mathrm{supp}(c)$ bevat. Alle q-secanten aan $\mathrm{supp}(c)$, die elk een q-secant vlak met de rechte $\langle T, R \rangle$ opspannen, snijden de rechte $\langle T, R \rangle$ in hetzelfde punt.*

Bewijs. Beschouw een codewoord $c \in \mathcal{C}_2(4,q)^\perp$ en $w(c) = q(q+2)+2$. We noteren $\mathrm{supp}(c)$ als $\mathcal{S}$. Stel dat er twee q-secanten n_1 en n_2 aan $\mathcal{S}$ bestaan die elk een q-secant vlak met de rechte $\langle T, R \rangle$ opspannen. We gaan er ook vanuit dat de rechte $\langle T, R \rangle$ geen punten van $\mathcal{S}$ bevat. Veronderstel dat de rechten n_1 en n_2 de rechte $\langle T, R \rangle$ respectievelijk snijden in de punten T_1 en T_2, maar dat $T_1 \neq T_2$. Merk op dat $T_1, T_2 \notin \mathcal{S}$, want de rechte $\langle T, R \rangle$ bevat geen punten van $\mathcal{S}$. In het vlak $\langle T_1, n_2 \rangle$ liggen alle punten van $\mathcal{S}$ op de q-secant n_2. Omdat $T_1 \notin n_2$, ligt het punt T_1 in dit vlak op q raaklijnen en één 0-secant. In het bijzonder volgt er uit Lemma 5.3.1 dat T_1 niet op de q-secant n_1 mag liggen. Dit geeft de verwachte strijdigheid en dus is $T_1 = T_2$. De stelling is bewezen omdat n_1 en n_2 willekeurige rechten zijn, die voldoen aan de voorwaarden van de stelling. ■

Stelling 5.3.5. *Gegeven een codewoord $c \in \mathcal{C}_2(4,q)^\perp$, $q = 8$, met $w(c) = q(q+2)+2$ en een punt $R \notin \mathrm{supp}(c)$ zodat de projectie van c uit R een hypercilinder $\mathcal{H}$ in een 3-ruimte is. Stel dat R op een 2-secant rechte $m = \langle P_1, P_2 \rangle$ ligt, met $P_1, P_2 \in \mathcal{S}$. Als de top T van de hypercilinder $\mathcal{H}$ op de rechte m ligt, dan gaan er $\frac{q}{2}+1$ verschillende $(q+1)$-secant rechten door het punt P_1 en $\frac{q}{2}+1$ verschillende $(q+1)$-secant rechten door het punt P_2.*

Bewijs. Neem een codewoord $c \in \mathcal{C}_2(4,q)^\perp$ met gewicht $q(q+2)+2$ en een punt R zoals in het gegeven. We noemen de rechten die de q-secanten worden van de hypercilinder $\mathcal{H}$ na projectie, de rechten l_i, met $i \in \{1,\ldots,q+2\}$. We weten hoe de punten van $\mathcal{S}$ liggen in elk vlak $\langle l_i, R\rangle$. In het vlak $\langle l_i, R\rangle$ ligt R op één 2-secant $\langle P_1, P_2\rangle$, met $P_1, P_2 \in \mathcal{S}$. De punten P_1 en P_2 worden geprojecteerd op de top T van $\mathcal{H}$. Omdat de rechte l_i een q-secant is van de hypercilinder volgt er via Lemma 5.3.1 dat de andere rechten door R in het vlak $\langle l_i, R\rangle$ raaklijnen zijn. Zo zien we ook dat $|\langle l_i, R\rangle \cap \mathcal{S}| = q+2$. Er volgt dan uit Lemma 5.3.3 dat de punten $(\mathcal{S} \cap \pi) \setminus \{P_1, P_2\}$ op een $(q+1)$-secant door P_1 of P_2 liggen. Dit geldt voor alle $i \in \{1,\ldots,q+2\}$, dus hebben we $q+2$ verschillende $(q+1)$-secant rechten gevonden die ofwel door het punt P_1 ofwel door het punt P_2 gaan. Via het duivenhokprincipe kunnen we zonder verlies van algemeenheid veronderstellen dat P_1 op minstens $\frac{q}{2}+1$ verschillende $(q+1)$-secant rechten ligt. Veronderstel dat P_1 op juist $\frac{q}{2}+1+\epsilon$ zo'n rechten ligt, met $\epsilon \geq 0$. Beschouw een hypervlak π dat de punten P_1 en P_2 niet bevat. Het hypervlak π bevat dan $q+2$ punten van $\mathcal{S}$, namelijk één van elke rechte l_i. Als we c beperken tot het hypervlak π, vinden we een codewoord met grootte $q+2$ van de code $\mathcal{C}_2(3,q)^\perp$. Uit de classificatie van de minimum gewicht codewoorden volgt dat deze $q+2$ punten een hyperovaal $\mathcal{O}$ vormen in een vlak van π. De hypercilinder $\mathcal{H}'$ met als basis $\mathcal{O}$ en top P_1 heeft minstens $q(\frac{q}{2}+1+\epsilon)$ punten gemeen met $\mathrm{supp}(c)$. Het codewoord van $\mathcal{C}_2(4,q)^\perp$ dat correspondeert met $\mathcal{H}'$ noteren we als c'. We bekijken het gewicht van het codewoord $c-c'$. Dit is niet nul, want het punt P_1 is bevat in $\mathrm{supp}(c)$, maar niet in $\mathrm{supp}(c')$. Dus is $w(c-c')$ minstens het minimum gewicht $q(q+2)$. Zo vinden we:

$$\begin{aligned} q(q+2) &\leq w(c-c') = w(c)+w(c')-2w(c\cap c') \\ \Rightarrow q(q+2) &\leq (q(q+2)+2)+q(q+2)-2q(\frac{q}{2}+1+\epsilon) \\ \iff 0 &\leq q(q+2)+2-q^2-2q-2q\epsilon \\ \iff 0 &\leq 2-2q\epsilon, \end{aligned}$$

dus is $\epsilon = 0$. Hieruit volgt dat er inderdaad $\frac{q}{2}+1$ verschillende $(q+1)$-secant rechten door het punt P_1 gaan. De overige $\frac{q}{2}+1$ verschillende $(q+1)$-secant rechten gaan bijgevolg door het punt P_2. ∎

We kunnen nu uitsluiten dat het punt R op een 2-secant rechte ligt.

Stelling 5.3.6. *Gegeven een codewoord $c \in \mathcal{C}_2(4,q)^\perp$, $q=8$, met $w(c) = q(q+2)+2$ en een punt $R \notin \mathrm{supp}(c)$ zodat de projectie van c uit R een hypercilinder is die een 3-ruimte opspant. Het is niet mogelijk dat het punt R op een 2-secant rechte ligt.*

Bewijs. Stel dat c een codewoord is van $\mathcal{C}_2(4,q)^\perp$ met gewicht $q(q+2)+2$. De support van c geven we weer via het symbool $\mathcal{S}$. Veronderstel dat R op een 2-secant $\langle P_1, P_2\rangle$, met $P_1, P_2 \in \mathcal{S}$, ligt. Het punt T is de top van de hypercilinder die we vinden na projectie. Veronderstel eerst dat $\langle T, R\rangle \neq \langle P_1, P_2\rangle$. Elk vlak door een q-secant van deze hypercilinder en het punt R bevat dan precies q punten van $\mathcal{S}$. Uit Lemma's 5.3.2 en 5.3.4 volgt dat de punten uit $\mathcal{S} \setminus \{P_1, P_2\}$ liggen op $q+2$ verschillende q-secant rechten door een punt $T' \in \langle T, R\rangle$. Merk op dat T' geen punt is van $\mathcal{S}$ omdat in dit geval de rechte $\langle T, R\rangle$ geen punten van $\mathcal{S}$ bevat. Het doel is om aan te tonen dat deze constructie een hypercilinder is. Er zijn in $\mathrm{PG}(4,q)$ juist θ_3 hypervlakken door T'. Dus zijn er q^4 hypervlakken die het punt T' niet bevatten. De punten P_1 en P_2 liggen elk ook in θ_3 hypervlakken. Samen zullen ze in θ_2 hypervlakken liggen. Hieruit volgt dat het aantal hypervlakken dat minstens één van beide punten P_1 of P_2 bevat gelijk is aan $2\theta_3 - \theta_2 = 2q^3+q^2+q+1$. Omdat $q>2$, is $q^4 > 2q^3+q^2+q+1$ en bestaat er dus een hypervlak π' dat de punten T', P_1 en P_2 niet bevat. Dit hypervlak bevat dan één punt van elk van de q-secant rechten door T'. Dus $|\pi' \cap \mathcal{S}| = q+2$. Ook is de beperking van c tot π' een codewoord van $\mathcal{C}_2(3,q)^\perp$. Uit de karakterisering van de minimum

gewicht codewoorden volgt er dat deze $q+2$ punten een hyperovaal $\mathcal{O}$ vormen in een vlak $\pi \subset \pi'$. We kunnen $\mathcal{O}$ dan beschouwen als basis en het punt T' als top voor een hypercilinder $\mathcal{H}$. Het is duidelijk dat onze $q+2$ verschillende q-secanten samen vallen met $\mathcal{H}$. We associëren het codewoord c' met $\mathcal{H}$. Dan heeft het codewoord $c - c'$ gewicht twee en $\text{supp}(c - c') = \{P_1, P_2\}$. Maar het minimum gewicht van $\mathcal{C}_2(4, q)^\perp$ is $q(q+2) > 2$, wat de beloofde strijdigheid geeft.

We moeten nu nog aantonen dat ook het geval $\langle T, R\rangle = \langle P_1, P_2\rangle$ een strijdigheid geeft. Via Stelling 5.3.5 weten we dat er $\frac{q}{2} + 1$ verschillende $(q+1)$-secanten gaan door elk van de punten P_1 en P_2. Neem een $(q+1)$-secant l door P_1. In het vlak $\langle l, R\rangle$ ligt het punt P_2 enkel op 2-secant rechten. We kiezen op één van deze rechten m verschillend van $\langle P_1, P_2\rangle$ een punt $R' \notin \mathcal{S}$. Het snijpunt van de rechten m en l noemen we P_1'. We kunnen de vorige stellingen toepassen met de punten R', P_1' en P_2 in plaats van R, P_1 en P_2. Zo vinden we dat ook P_1' op $\frac{q}{2} + 1$ verschillende $(q+1)$-secanten ligt. Door een hypervlak π' te nemen waar P_1 en P_2 niet inliggen, zien we dat er een vlak $\pi \subset \pi'$ bestaat waarin $\mathcal{S}$ een hyperovaal is. Stel dat we vanuit het punt P_1 projecteren op het hypervlak π'. Dan vinden we dat de $(q+1)$-secanten door P_1 projecteren op een $(\frac{q}{2} + 1)$-boog van deze hyperovaal in π. Dus ook het punt P_1' wordt geprojecteerd op een punt van de $(\frac{q}{2} + 1)$-boog. Stel dat n een $(q+1)$-secant rechte door P_1' is, met $n \neq \langle P_1, P_1'\rangle$. Omdat P_1 niet op de rechte n ligt, wordt n geprojecteerd vanuit P_1 op een rechte n' in het hypervlak π'. De rechte n' mag hoogstens twee punten van de $(\frac{q}{2} + 1)$-boog bevatten. Hieruit volgt dat de rechte n hoogstens twee punten bevat van $(q+1)$-secanten door P_1. Dus moet de $(q+1)$-secant n door P_1' minstens $q-1$ punten bevatten van $(q+1)$-secanten door P_2. Maar n bevat hoogstens één punt van elke $(q+1)$-secant door P_2. Dit geeft een strijdigheid, want er zijn zo maar $\frac{q}{2} + 1$ rechten door P_2. Hieruit volgt dat de 2-secant $\langle P_1, P_2\rangle$ niet bestaat. ■

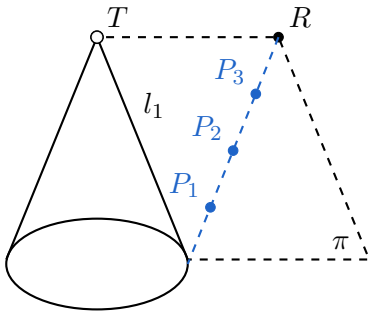
Er blijft dus maar één mogelijkheid over: het punt R ligt op één 3-secant aan $\mathcal{S}$. We kunnen echter ook deze mogelijkheid en bijgevolg het bestaan van een codewoord met gewicht $q(q+2)+2$ in de code $\mathcal{C}_{n-2}(n, 8)^\perp$ uitsluiten.

Stelling 5.3.7. *Er bestaat geen codewoord $c \in \mathcal{C}_{n-2}(n, q)^\perp$, met $q = 8$, zodat $w(c) = q(q+2)+2$.*

Bewijs. Neem een codewoord $c \in \mathcal{C}_{n-2}(n, q)^\perp$ met gewicht $q(q+2)+2$. We noteren $\text{supp}(c)$ als $\mathcal{S}$. Uit Gevolg 5.2.8 volgt dat $\mathcal{S}$ bevat is in een 4-ruimte ρ. Via eventueel meerdere keren te projecteren, vinden we dat $c \in \mathcal{C}_2(4, q)^\perp$. Daarnaast weten we dat er een punt $R \notin \mathcal{S}$ ligt in de 4-ruimte ρ zodat de projectie vanuit R een hypercilinder $\mathcal{H}$ is die een 3-ruimte opspant. Dit punt R ligt dan op minstens één raaklijn, omdat $\mathcal{H}$ bestaat uit $q(q+2)$ punten en $w(c) = q(q+2)+2$. Uit Stellingen 5.3.1 en 5.3.6 volgt dat R op één 3-secant rechte aan $\mathcal{S}$ ligt. Stel dat deze 3-secant wordt voortgebracht door de punten P_1, P_2 en P_3 van $\mathcal{S}$. We noemen de q-secant rechten van de hypercilinder $\mathcal{H}$ de rechten l_i, met $i \in \{1, \ldots, q+2\}$. De rechte $\langle P_1, P_2, P_3\rangle$ wordt vanuit R geprojecteerd op een punt, verschillend van T, van een rechte l_i. Zonder verlies van algemeenheid veronderstellen we dat dit l_1 is. We geven deze configuratie weer in Figuur 5.3. De vlakken $\langle l_i, R\rangle$, $i \neq 1$, bevatten allemaal q punten van $\mathcal{S}$. Het "unieke" vlak $\langle l_1, R\rangle$ dat $q+2$ punten van $\mathcal{S}$ bevat noemen we π. In het vlak π zullen we een strijdigheid vinden. Een gelijkaardige redenering hebben we in het bewijs van Stelling 5.3.3 gebruikt.

In π ligt het punt R op één 0-secant namelijk, de rechte $\langle T, R\rangle$, één 3-secant namelijk, de rechte $\langle P_1, P_2\rangle$, en voor het overige op raaklijnen. Neem een willekeurig ander punt R' op de rechte $\langle P_1, P_2\rangle$ zodat R' niet tot $\mathcal{S}$ behoort. Als we zouden projecteren uit R' vinden we een niet-nul codewoord, maar we verliezen we wel al minstens twee punten. Deze projectie moet dus een hypercilinder zijn. In het bijzonder volgt er dat R' naast de 3-secant rechte $\langle P_1, P_2\rangle$ in het vlak π voor de rest op $q-1$ raaklijnen en één 0-secant ligt. Neem nu een punt $R' \notin \mathcal{S}$ dat niet op de rechte $\langle T, R\rangle$ of $\langle P_1, P_2\rangle$ ligt. Dit punt ligt dan op de raaklijn $\langle R, R'\rangle$. Uit Lemma 5.3.1 en het feit dat $|\pi \cap \mathcal{S}| = q+2$,

volgt dat R' op één secant, hoogstens één 0-secant en voor het overige op raaklijnen ligt in het vlak π. We hebben dus bewezen dat een rechte door een punt $R' \in \pi \setminus \langle T, R\rangle$, met $R' \notin \mathcal{S}$, hoogstens drie punten van $\mathcal{S}$ bevat en dat R' op precies één secant ligt. Neem een punt $P_4 \in (\pi \cap \mathcal{S}) \setminus \{P_1, P_2, P_3\}$. Merk op dat P_4 niet op de rechte $\langle P_1, P_2\rangle$ kan liggen. Elke rechte m door P_4 in π snijdt de rechte $\langle T, R\rangle$ in een punt $Q \notin \mathcal{S}$. Als de rechte m een q-secant is, dan bevat deze zonder verlies van algemeenheid het punt P_1, maar niet P_2 en P_3. Het punt Q ligt op minstens twee raaklijnen in π, namelijk $\langle Q, P_2\rangle$ en $\langle Q, P_3\rangle$. Lemma 5.3.1 toepassen op Q geeft dan een strijdigheid, want m bevat teveel punten van $\mathcal{S}$. Dus de rechte m bevat minstens één punt $R' \notin \mathcal{S}$ zodat $R' \notin \langle T, R\rangle$. Uit onze eerder observatie volgt dat m hoogstens een 3-secant is. Omdat dit geldt voor alle rechten door het punt P_4 volgt uit het duivenhokprincipe dat P_4 op minstens $\frac{q}{2} + 1$ verschillende secanten ligt in π. Dit betekent dat er minstens één hiervan de rechte $\langle P_1, P_2\rangle$ snijdt in een punt R' verschillend van P_1, P_2, P_3 of $R = \langle P_1, P_2\rangle \cap \langle T, R\rangle$. Het punt R' behoort dan niet tot $\mathcal{S}$, maar ligt wel op twee verschillende secanten: $\langle R', P_4\rangle$ en $\langle P_1, P_2\rangle$. Dit geeft opnieuw een strijdigheid. Dus ook de mogelijkheid dat R op een 3-secant ligt is uitgesloten. Hiermee is de stelling bewezen. ■



Figuur 5.3.: De hypercilinder $\mathcal{H}$ met top T die we vinden via projectie vanuit het punt R. In stippellijnen duiden we het vlak $\pi = \langle R, l_1\rangle$ aan, hierin is l_1 na de projectie een q-secant van $\mathcal{H}$. Het vlak π bevat ook een 3-secant rechte $\langle P_1, P_2\rangle$ aan $\mathcal{S}$ door R, met $P_1, P_2, P_3 \in \mathcal{S}$.

5.4. Geen codewoord met gewicht $q^{n-k-1}(q+2)+2$ in $\mathcal{C}_k(n,8)^\perp$

Uit het vorige deel weten we dat er geen codewoord bestaat met gewicht $q(q+2)+2$ in de code $\mathcal{C}_{n-2}(n,8)^\perp$. Hieruit kunnen we afleiden dat er geen codewoord $c \in \mathcal{C}_k(n,8)^\perp$ bestaat met gewicht $q^{n-k-1}(q+2)+2$ voor $k \in \{1, \ldots, n-3\}$.

Stelling 5.4.1. *Er bestaat geen codewoord $c \in \mathcal{C}_k(n,8)^\perp$ met gewicht $q^{n-k-1}(q+2)+2$ als $k \in \{1, \ldots, n-2\}$.*

Bewijs. Dankzij Stelling 5.3.7 weten we dat de stelling waar is voor $k = n-2$. Dit zullen we gebruiken om de stelling te bewijzen voor $k < n-2$. Stel dat c een codewoord is van $\mathcal{C}_k(n,q)^\perp$ met $w(c) = q^{n-k-1}(q+2)+2$ en $k < n-2$. We noteren $\mathrm{supp}(c)$ korter als $\mathcal{S}$. Het doel is om een $(k+2)$-ruimte te construeren waar $q(q+2)+2$ punten van $\mathcal{S}$ in liggen. Door c te beperken tot deze deelruimte zullen we dan een strijdigheid vinden. We beginnen onze constructie met een punt $P \in \mathcal{S}$ te kiezen. We willen Stelling 3.1.4 toepassen om een $(k-1)$-ruimte τ_{k-1} te vinden zodat $\tau_{k-1} \cap \mathcal{S} = \{P\}$. Omdat de ongelijkheid

$$q^{n-k-1}(q+2)+2 = q^{n-k} + 2q^{n-k-1} + 2 \leq 2q^{n-k}$$

waar is voor $q = 8$ en onze waarden van k, mogen we Stelling 3.1.4 gebruiken. Zo vinden we een $(k-1)$-ruimte τ_{k-1} die enkel het punt P van $\mathcal{S}$ bevat. Door τ_{k-1} zijn er θ_{n-k} verschillende

k-ruimten τ_k. Deze bevatten elk minstens één extra punt van $\mathcal{S}$ opdat $(c, \tau_k) = 0$. Er bestaat ook minstens één τ_k die juist één extra punt bevat van $\mathcal{S}$. Dit kunnen we inzien door de punten van $\mathcal{S}$ te tellen. Als dit niet waar is, zijn er minstens $2\theta_{n-k}$ extra punten van $\mathcal{S}$ nodig. Dit geeft een strijdigheid, want:

$$q^{n-k-1}(q+2) + 2 - 1 = q^{n-k-1}(q+2) + 1 \leq 2q^{n-k} < 2\theta_{n-k}.$$

Dus stel dat τ_k een k-ruimte door τ_{k-1} is die precies twee punten P en Q van $\mathcal{S}$ bevat. We bekijken nu een $(k+1)$-ruimte door τ_k. Daarin zijn q verschillende k-ruimten door τ_{k-1} bevat naast τ_k. Deze moeten allemaal minstens één extra punt van $\mathcal{S}$ bevatten. Ook is het totale aantal punten van $\mathcal{S}$ in een k-ruimte even. Dus een $(k+1)$-ruimte door τ_k bevat q of minstens $q+2$ extra punten van $\mathcal{S}$. Er zijn θ_{n-k-1} verschillende $(k+1)$-ruimten door τ_k. Deze bevatten niet allemaal minstens $q+2$ extra punten van $\mathcal{S}$, want de volgende ongelijkheid is waar:

$$\begin{aligned} &|\mathcal{S}| - 2 = q^{n-k-1}(q+2) + 2 - 2 < (q+2) \cdot (q^{n-k-1} + q^{n-k-2} + \cdots + 1) \\ \iff &q^{n-k} + 2q^{n-k-1} < (q^{n-k} + q^{n-k-1} + \cdots + q) + (2q^{n-k-1} + 2q^{n-k-2} + \cdots + 2) \\ \iff &0 < q^{n-k-1} + 3q^{n-k-2} + \cdots + 3q + 2. \end{aligned}$$

Stel dus dat τ_{k+1} een $(k+1)$-ruimte door τ_k is zodat $|\tau_{k+1} \cap \mathcal{S}| = q+2$. We bekijken nu de $(k+2)$-ruimten door τ_{k+1}. In het algemeen geldt er dat als we c beperken tot een $(k+2)$-ruimte τ_{k+2} we een codewoord van $\mathcal{C}_k(k+2, q)^\perp$ vinden. Dit betekent dat τ_{k+2} precies $q(q+2)$ of minstens $q(q+2)+4$ punten van $\mathcal{S}$ bevat. In het bijzonder bevat elke $(k+2)$-ruimte door τ_{k+1} minstens $q(q+2) - (q+2) = (q-1)(q+2)$ extra punten van $\mathcal{S}$. Omdat er θ_{n-k-2} verschillende mogelijkheden zijn voor τ_{k+2}, vinden we zo al minstens

$$(q+2) + \theta_{n-k-2}(q-1)(q+2) = q^{n-k-1}(q+2)$$

punten van $\mathcal{S}$. Er blijven juist twee punten van $\mathcal{S}$ over. Dus één $(k+2)$-ruimte door τ_{k+1} bevat precies $q(q+2)+2$ punten van $\mathcal{S}$. Dit geeft echter een strijdigheid met Stelling 5.3.7. We besluiten dat er geen codewoord $c \in \mathcal{C}_k(n, q)^\perp$ bestaat met $w(c) = q^{n-k-1}(q+2) + 2$. ■

Gevolg 5.4.2. *Er bestaat geen codewoord $c \in \mathcal{C}_k(n, 8)^\perp$ met gewicht in het open interval*

$$]q^{n-k-1}(q+2), q^{n-k-1}(q+2) + 4[$$

voor $k \in \{1, \ldots, n-2\}$.

Bewijs. Dit volgt uit Stellingen 5.1.1 en 5.4.1. ■

Hiermee hebben we het hoofdresultaat van dit hoofdstuk bewezen. In de mate van het mogelijke hebben we de argumenten zoveel mogelijk onafhankelijk gemaakt van $q = 8$. Indien ook voor grotere even q bewezen wordt dat de minimum gewicht codewoorden hypercilinders zijn, kan men dan hopelijk sneller de resultaten over de codewoorden met gewicht in bovenstaand interval uitbreiden. In het volgende en laatste hoofdstuk geven we voorbeelden van enkele andere incidentiecodes.

6 Gerelateerde codes

In dit hoofdstuk geven we voorbeelden van codes die lijken op de code $\mathcal{C}_k(n,q)$. We beginnen met wat meer informatie te geven over de code $\mathcal{C}_{j,k}(n,q)$ en zijn duale. Daarna vermelden we twee andere relevante codes. Ter illustratie bespreken we enkele codewoorden met een klein gewicht voor specifieke parameterwaarden van deze codes. We zullen ook de term klassieke polaire ruimten gebruiken. Hiermee bedoelen we elliptische, parabolische, hyperbolische kwadrieken, Hermitische variëteiten of symplectische ruimten. We gaan er ook steeds vanuit dat als we één van deze polaire ruimten vermelden, dat deze niet-singulier zijn.

6.1. Code van deelruimten

In de vorige hoofdstukken hebben we het minimum gewicht en codewoorden met een klein gewicht van $\mathcal{C}_{j,k}(n,q)$ en $\mathcal{C}_{j,k}(n,q)^\perp$ bestudeerd voor $j=0$. We kunnen ons nu afvragen wat er nog geweten is voor $j \geq 0$. De bespreking hiervan doen we niet in detail, maar we vermelden hier enkele resultaten en recente artikels. Bagchi en Inamdar hebben bewezen dat het minimum gewicht van $\mathcal{C}_{j,k}(n,q)$ gelijk is aan $\begin{bmatrix} k+1 \\ j+1 \end{bmatrix}_q$ in [8, Theorem 1]. Deze minimum codewoorden zijn de scalaire veelvouden van de k-ruimten [8]. De codewoorden tot een bepaald gewicht zijn ook gekarakteriseerd. De recentste artikels hierover zijn van Adriaensen en Denaux: [2] en [3]. Voor q voldoende groot, tonen ze eerst aan dat elk codewoord met hoogstens gewicht $\left(3-\frac{7}{q}\right)\begin{bmatrix} k+1 \\ j+1 \end{bmatrix}_q$ een lineaire combinatie is van hoogstens twee k-ruimten [2, Theorem 6.7]. Ook voor kleinere q geven Adriaensen en Denaux een karakterisering tot een bepaald gewicht. De details hiervan kan men nagaan in [2, Theorem 6.7]. Dezelfde auteurs hebben vervolgens in [3] verdere karakteriseringsresultaten bewezen. Daarnaast geven Adriaensen en Denaux in dit artikel ook een mooi historisch overzicht van belangrijke resultaten over $\mathcal{C}_{j,k}(n,q)^\perp$. We geven hier zonder bewijs het hoofdresultaat van [3].

Stelling 6.1.1. *[3, Theorem 1.6] Gegeven is $q=p^h$ met $q \geq 32$ en $h \in \mathbb{N} \setminus \{0,1\}$. Stel dat het codewoord $c \in \mathcal{C}_{j,k}(n,q)$ gewicht $w(c)$ heeft met*

$$w(c) \leq \begin{cases} \left(\frac{1}{2}\sqrt{q}-\frac{7}{2}\right)\begin{bmatrix} k+1 \\ j+1 \end{bmatrix}_q & \text{als } h=2, \\ \left\lfloor \sqrt{q}-\frac{3}{2} \right\rfloor \begin{bmatrix} k+1 \\ j+1 \end{bmatrix}_q & \text{anders,} \end{cases}$$

dan is c een lineaire combinatie van juist $\left\lceil \frac{w(c)}{\begin{bmatrix} k+1 \\ j+1 \end{bmatrix}_q} \right\rceil$ karakteristieke vectoren van k-ruimten.

Het minimum gewicht van $\mathcal{C}_{j,k}(n,q)^\perp$ is in het algemeen niet gekend. Echter in [2, Corollary 7.10] hebben Adriaensen en Denaux bewezen dat $d(\mathcal{C}_{j,k}(n,q)^\perp) = d(\mathcal{C}_{0,1}(n-k+1,q)^\perp)$. Dus voor q priem en q even weten we dat het minimum gewicht respectievelijk $2q^{n-k}$ en $(q+2)q^{n-k-1}$ is. Het blijkt dat de minimum gewicht codewoorden van $\mathcal{C}_{j,k}(n,q)^\perp$ geconstrueerd worden via codewoorden van $\mathcal{C}_{0,k-j}(n-j,q)^\perp$, zie [2] voor meer informatie hierover.

In hetzelfde artikel is ook de doorsnede $\mathcal{C}_{j,k}(n,q) \cap \mathcal{C}_{j,n-k+j}(n,q)^\perp$ besproken. Herinner dat wij deze code hebben bekeken voor $j = 0$ om te bewijzen dat er een leeg interval is in de gewichten van de code $\mathcal{C}_k(n,q)$. In [2, Theorem 6.7] wordt aangetoond dat voor de meeste q de minimum gewicht codewoorden van $\mathcal{C}_{j,k}(n,q) \cap \mathcal{C}_{j,n-k+j}(n,q)^\perp$ scalaire veelvouden zijn van het verschil van twee k-ruimten door een $(k-1)$-ruimte. Voor verdere details en andere resultaten verwijzen we de geïnteresseerde lezer naar [2].

6.2. Code van snijdende rechten

Wij hebben de code $\mathcal{C}_{j,k}(n,q)$ gedefinieerd via een specifieke incidentiematrix G. Herinner dat $0 \leq j < k < n$. Elke rij van G correspondeert met een k-ruimte σ en elke kolom met een j-ruimte τ. We definieerden $G_{\tau,\sigma} = 1$ als $\sigma \subset \tau$ en anders is $G_{\tau,\sigma} = 0$. We zouden onze incidentiematrix echter ook op een andere manier kunnen definiëren. De voorwaarden op j en k zijn dan ook anders: $0 \leq j, k < n$. Opnieuw corresponderen onze kolommen met de j-ruimten en de rijen met de k-ruimten in $\mathrm{PG}(n,q)$. We werken ook nog steeds over $\mathbb{F}_p$. Maar nu plaatsen we een 1 als de j-ruimte een niet lege intersectie heeft met de k-ruimte. In de literatuur noteert men deze code ook als $\mathcal{C}_{j,k}(n,q)$, maar om verwarring te vermijden zullen wij $\mathcal{M}_{j,k}(n,q)$ gebruiken. Echter als $j = 0$ en $k > 0$, dan is $\mathcal{M}_{0,k}(n,q)$ dezelfde code als $\mathcal{C}_{0,k}(n,q)$. Als $j = 0$ en $k = 0$ vinden we dat G de identiteitsmatrix is. Wat is er al geweten over het minimum gewicht, de dimensie en de lengte van de code $\mathcal{M}_{j,k}(n,q)$? Het bepalen van het minimum gewicht van de code $\mathcal{M}_{j,k}(n,q)$ is nog een open probleem voor $j, k > 0$ en $j + k \leq n - 1$ [6]. De dimensie is wel gekend. Dit is bewezen door Sin in [36]. Daarnaast is het duidelijk dat de lengte van $\mathcal{M}_{j,k}(n,q)$ gelijk is aan $\begin{bmatrix} n+1 \\ j+1 \end{bmatrix}_q$. We zullen de codewoorden met een klein gewicht van de code $\mathcal{M}_{j,k}(n,q)$ in meer detail bestuderen voor $j = k = 1$ en $n = 3$.

De resultaten over $\mathcal{M}_{1,1}(3,q)$ die we bespreken, zijn bewezen door Adriaensen, Simoens en Storme in [6]. We volgen hieronder hun aanpak. Het doel is om de codewoorden van $\mathcal{M}_{1,1}(3,q)$ met gewicht ten hoogste $q^3 + 2q^2 + q + 1$ te karakteriseren. De eerste stap is bewijzen dat de karakteristieke vector van de rechten van een symplectische polaire ruimte $W(3,q)$ een codewoord is van $\mathcal{M}_{1,1}(3,q)$ als en slechts als q even is. Hiervoor moeten we hier op een andere manier de karakteristieke vector van een k-ruimte definiëren zodat deze beter past bij de code $\mathcal{M}_{j,k}(n,q)$. In dit deel bedoelen we met de karakteristieke vector van een k-ruimte dus onderstaande definitie zoals in [6].

Definitie 6.2.1 (Karakteristieke vector van een k-ruimte). De karakteristieke vector $\chi_\tau^{(j)}$ van een k-ruimte τ is de karakteristieke vector van de verzameling j-ruimten die τ snijden in minstens één punt.

Dit betekent dat de karakteristieke vector $\chi_\tau^{(j)}$ van de k-ruimte τ overeenkomt met de rij G_τ van de code $\mathcal{M}_{j,k}(n,q)$. We zouden onze code dus equivalent kunnen definiëren via deze karakteristieke vectoren. Dit is de manier waarop de code $\mathcal{M}_{j,k}(n,q)$ gedefinieerd is in [6]. Merk op dat daar niet toegelaten is dat j of k nul is. De verzameling van alle j-ruimten in $\mathrm{PG}(n,q)$ noteren we als

$\mathcal{G}_j(n,q)$. We kunnen onze codewoorden ook zien als afbeeldingen $c : \mathcal{G}_j(n,q) \to \mathbb{F}_p$. Hieruit kunnen we via een nieuwe soort van projectie andere afbeeldingen halen.

Definitie 6.2.2 (Projectie afbeelding). [6, Definition 4.1] Beschouw de getallen $0 < i < j < n$ en een afbeelding $c : \mathcal{G}_j(n,q) \to \mathbb{F}_p$. We definiëren de afbeelding $\mathrm{proj}^{(i)}(c)$ als volgt:

$$\mathrm{proj}^{(i)}(c) : \mathcal{G}_i(n,q) \to \mathbb{F}_p : \rho \to \sum_{\substack{\tau \in \mathcal{G}_j(n,q) \\ \rho \subseteq \tau}} c_\tau.$$

We gebruiken de notatie ${\mathbb{F}_p}^{\mathcal{G}_j(n,q)}$ voor de vectorruimte waarin de code $\mathcal{M}_{j,k}(n,q)$ en zijn duale code $\mathcal{M}_{j,k}(n,q)^\perp$ leven, $\forall k \in \{1,\ldots,n-1\}$. Neem een vector $c \in {\mathbb{F}_p}^{\mathcal{G}_j(n,q)}$. De afbeelding $\mathrm{proj}^{(i)}(c)$ komt overeen met een vector in ${\mathbb{F}_p}^{\mathcal{G}_i(n,q)}$. We kunnen aantonen dat $c \in \mathcal{M}_{j,k}(n,q)^\perp$ als en slechts als $\mathrm{proj}^{(i)}(c) \in \mathcal{M}_{i,k}(n,q)^\perp$. Dit zullen we gebruiken om te bewijzen dat de karakteristieke vector van een symplectische polaire ruimte $W(2n+1,q)$ een codewoord is van $\mathcal{M}_{1,n}(2n+1,q)$ als en slechts als q even is.

Lemma 6.2.3. *[6, Lemma 4.3] Beschouw een vector $c \in {\mathbb{F}_p}^{\mathcal{G}_j(n,q)}$ en getallen $0 < i,j,k < n$, met $i < j$. De vector c is een codewoord van $\mathcal{M}_{j,k}(n,q)^\perp$ als en slechts als $\mathrm{proj}^{(i)}(c)$ een codewoord is van $\mathcal{M}_{i,k}(n,q)^\perp$.*

Bewijs. Veronderstel dat c een vector is van ${\mathbb{F}_p}^{\mathcal{G}_j(n,q)}$. De vector $\mathrm{proj}^{(i)}(c)$ behoort tot $\mathcal{M}_{i,k}(n,q)^\perp$ als en slechts als deze orthogonaal is met alle vectoren van de incidentiematrix. De voorwaarde is dus dat voor alle k-ruimten κ geldt:

$$0 = \mathrm{proj}^{(i)}(c) \cdot \chi_\kappa^{(i)} = \sum_{\rho \in \mathcal{G}_i(n,q)} \mathrm{proj}^{(i)}(c)_\rho \cdot \mathbb{1}_{\rho \cap \kappa \neq \emptyset} = \sum_{\substack{\rho \in \mathcal{G}_i(n,q) \\ \rho \cap \kappa \neq \emptyset}} \mathrm{proj}^{(i)}(c)_\rho = \sum_{\substack{\rho \in \mathcal{G}_i(n,q) \\ \rho \cap \kappa \neq \emptyset}} \sum_{\substack{\tau \in \mathcal{G}_j(n,q) \\ \rho \subseteq \tau}} c_\tau.$$

Hierboven hebben we eerst de definitie van de karakteristieke vector van κ gesubstitueerd en zo onze som herschreven. Nadien gebruiken we de definitie van $\mathrm{proj}^{(i)}(c)_\rho$. Nu kunnen we bovenstaande som verder vereenvoudigen. We bekijken immers alle j-ruimten τ die door een i-ruimte ρ gaan. We doen dit voor alle i-ruimten die een niet lege intersectie hebben met de vaste k-ruimte κ. Hieruit volgt dat we enkel de bijdrage bekijken van j-ruimten τ die ook een niet lege intersectie hebben met κ. We kunnen ons nu afvragen hoeveel keer we dezelfde j-ruimte τ tellen. Het aantal i-ruimten dat een niet lege intersectie heeft met $\tau \cap \kappa$ en bevat is in τ, is $1 \pmod p$. Dit is een gekend resultaat, zie bijvoorbeeld [11, Lemma 3.2]. Hieruit volgt dat we elke j-ruimte τ die κ snijdt juist één keer tellen modulo p. We kunnen bovenstaande som dus vereenvoudigen:

$$\sum_{\substack{\rho \in \mathcal{G}_i(n,q) \\ \rho \cap \kappa \neq \emptyset}} \sum_{\substack{\tau \in \mathcal{G}_j(n,q) \\ \rho \subseteq \tau}} c_\tau = \sum_{\substack{\tau \in \mathcal{G}_j(n,q) \\ \tau \cap \kappa \neq \emptyset}} c_\tau = c \cdot \chi_\kappa^{(j)}.$$

Het rechterlid is nul voor alle k-ruimten κ als en slechts als $c \in \mathcal{M}_{j,k}(n,q)^\perp$. Hiermee hebben we de stelling bewezen. ∎

Stelling 6.2.4. *[6, Proposition 4.4] Veronderstel dat $\mathcal{S}$ de verzameling is van de absolute rechten van een symplectische polariteit $W(2n+1,q)$ in $\mathrm{PG}(2n+1,q)$, met $n \geq 1$. De karakteristieke vector $\chi_\mathcal{S}$ is een codewoord van $\mathcal{M}_{1,n}(2n+1,q)$ als en slechts als q even is.*

Bewijs. We veronderstellen eerst dat q even is. We tonen aan dat de vector $\chi_{\mathcal{S}}$ zoals in het gegeven een codewoord is van de code $\mathcal{M}_{1,n}(2n+1,q)$. Neem een hyperbolische kwadriek $Q^+(2n+1,q)$ in $\mathrm{PG}(n,q)$. We noteren de verzameling bestaande uit de generatoren van één equivalentieklasse van $Q^+(2n+1,q)$ als $\mathcal{R}$. Beschouw de vector $c = \sum_{\tau\in\mathcal{R}} \chi_\tau^{(1)}$. Dan is c een codewoord van $\mathcal{M}_{1,n}(2n+1,q)$, want het is een som van rijen uit de incidentiematrix. We zullen bewijzen dat $c = \chi_{\mathcal{S}}$, zodat ook $\chi_{\mathcal{S}} \in \mathcal{M}_{1,n}(2n+1,q)$. Neem een rechte l uit $\mathrm{PG}(2n+1,q)$. De coëfficiënt c_l is gelijk aan het aantal generatoren in $\mathcal{R}$ die minstens één punt met l gemeen hebben. Stel dat l juist x verschillende punten met $Q^+(2n+1,q)$ gemeen heeft. Het aantal generatoren door een punt P dat op de rechte l, maar niet op de kwadriek ligt, is logischerwijs nul. Stel dat P wel op de hyperbolische kwadriek ligt. De generatoren door P liggen in de raakkegel door P. Deze kegel is van de vorm $PQ^+(2n-1,q)$. Elke generator van $Q^+(2n-1,q)$ geeft aanleiding tot een generator door P. We vinden dus $2\Pi_{i=1}^{n-1}(q^i+1)$ verschillende generatoren door het punt P. Als $n=1$, gaan we er vanuit dat dit lege product gelijk is aan één. De helft hiervan zal behoren tot de equivalentieklasse $\mathcal{R}$. Het aantal generatoren door de rechte l noteren we als y. We tellen het aantal generatoren die de rechte l minstens snijden, via de punten op l. Hierbij moeten we opletten dat we de generatoren die l volledig bevatten niet $q+1$ keer tellen. Wanneer we hiervoor corrigeren, vinden we:

$$c_l = x \cdot \prod_{i=1}^{n-1}(q^i+1) - qy = x \pmod p.$$

Nu kan de rechte l enkel 0, 1, 2 of $q+1$ punten van $Q^+(2n+1,q)$ bevatten. Omdat we hier modulo 2 werken, vinden we dat $c_l = 1$ als l een raaklijn is of bevat is in de kwadriek. Anders is $c_l = 0$. Aangezien q even is, is de polariteit die hoort bij de kwadriek een symplectische polariteit, zie de cursus Galoismeetkunde [39]. We willen graag de volgende eigenschap van symplectische polariteiten gebruiken: een rechte m is absoluut t.o.v. deze polariteit als en slechts als er een punt $P \in m$ is zodat $m \subset P^\perp$. De heenrichting is onmiddellijk duidelijk, want $P \in m \Rightarrow m^\perp \subset P^\perp$. Voor de omgekeerde richting veronderstellen we dat $P \in m$ en $m \subset P^\perp$. Neem een willekeurig punt van $Q \in m$ dat verschillend is van P. Uit het gegeven volgt dat $Q \in P^\perp$. Bijgevolg is $P \in Q^\perp$. Omdat we werken met een symplectische polariteit is $Q \in Q^\perp$, zodat ook $m = \langle P, Q\rangle \subset Q^\perp$. Aangezien $m^\perp = \bigcap_{Q\in m} Q^\perp$, besluiten we dat $m \subseteq m^\perp$. Uit deze eigenschap volgt dat enkel rechten die een niet-nul coëfficiënt hebben in c, absolute rechten zijn. Inderdaad, alle rechten door een punt P in zijn raakhypervlak $P^\perp$ zijn ofwel raaklijnen ofwel volledig bevat in de kwadriek. Hierdoor is c de karakteristieke vector van de absolute rechten van een symplectische polariteit. Dit is wat we wilden bewijzen.

Stel nu dat q oneven is. We tonen aan dat $\chi_{\mathcal{S}}$ geen codewoord van $\mathcal{M}_{1,n}(2n+1,q)$ is door een codewoord c in de duale code te maken zodat $c \cdot \chi_{\mathcal{S}} \neq 0$. We noteren de polariteit geassocieerd met de symplectische ruimte $W(2n+1,q)$ uit het gegeven als $\perp$. We gaan er vanuit dat deze de standaardvorm $b(X,Y) = \sum_{i=0}^{n}(X_{2i}Y_{2i+1} - X_{2i+1}Y_{2i})$, heeft. Anders zetten we de polariteit z.v.v.a. via een basistransformatie om naar de standaardvorm. Als $n=1$ stelt de deelruimte τ de hele ruimte $\mathrm{PG}(3,q)$ voor. Voor $n>1$ wordt de 3-ruimte τ bepaald door $X_4 = X_5 = \cdots = X_{2n+1} = 0$. Dan is $\tau^\perp$ de deelruimte met vergelijking $X_0 = X_1 = X_2 = X_3 = 0$. In het bijzonder is $\tau \cap \tau^\perp = \emptyset$. We kunnen $\perp$ beperken tot τ en vinden zo een $W(3,q)$. Beschouw ook een hyperbolische kwadriek $Q^+(3,q)$ in τ met bijhorende reguli $\mathcal{R}^+$ en $\mathcal{R}^-$. We definiëren als volgt een vector c geïndexeerd over de rechten van $\mathrm{PG}(2n+1,q)$:

$$c_m = \begin{cases} 1 & \text{als } m \in \mathcal{R}^+, \\ -1 & \text{als } m \in \mathcal{R}^-, \\ 0 & \text{anders.} \end{cases}$$

Om in te zien dat $c \in \mathcal{M}_{1,n}(2n+1,q)^\perp$, bekijken we $\mathrm{proj}^{(0)}(c)$. Neem een punt $P \in \mathrm{PG}(2n+1,q)$. Stel dat P op een rechte m van een regulus ligt, z.v.v.a. $m \in \mathcal{R}^+$. Dan ligt P ook op juist één rechte van de tegengestelde regulus. Hieruit volgt dat de coëfficiënt $\mathrm{proj}^{(0)}(c)_P = 0$. Als P niet op een rechte van de kwadriek ligt, is ook $\mathrm{proj}^{(0)}(c)_P = 0$. Dus is de vector $\mathrm{proj}^{(0)}(c)$ de nulvector en deze behoort duidelijk tot $\mathcal{M}_{0,n}(2n+1,q)^\perp$. Uit Lemma 6.2.3 volgt dat $c \in \mathcal{M}_{1,n}(2n+1,q)^\perp$. Als $\chi_\mathcal{S} \in \mathcal{M}_{1,n}(2n+1,q)$, dan zou $\chi_\mathcal{S} \cdot c = 0$. De definitie van c impliceert dat dit enkel kan als de verzameling $\mathcal{S}$ evenveel rechten van de twee reguli $\mathcal{R}^+$ en $\mathcal{R}^-$ bevat modulo p. We tonen aan dat dit niet steeds het geval is. We geven de symplectische polariteit in $\mathrm{PG}(3,q)$ weer als:

$$b(X,Y) = X_0Y_1 - X_1Y_0 + X_2Y_3 - X_3Y_2.$$

Vanaf nu is $\perp$ de bijhorende polariteit. We definiëren een hyperbolische kwadriek $Q^+(3,q)$ via de vergelijking $X_0X_1 = X_2X_3$. Uit het bewijs van de stelling van Gallucci, zie de oefeningen van galoismeetkunde, kunnen we de vorm van de generatoren van $Q^+(3,q)$ afleiden. Rekening houdend dat we werken met homogene coördinaten, vinden we zo

$$\begin{aligned}\mathcal{R}^+ &= \{\langle(\alpha,0,\beta,0),(0,\beta,0,\alpha)\rangle \mid\mid \langle(\alpha,\beta)\rangle \in \mathrm{PG}(1,q)\},\\ \mathcal{R}^- &= \{\langle(\alpha,0,0,\beta),(0,\beta,\alpha,0)\rangle \mid\mid \langle(\alpha,\beta)\rangle \in \mathrm{PG}(1,q)\}.\end{aligned}$$

We kunnen nu berekenen hoeveel absolute rechten $\mathcal{R}^+$ en $\mathcal{R}^-$ bevatten. Uit onze eerdere opmerking volgt dat het voldoende is om te controleren of de twee punten die de rechte opspannen in elkaars raakhypervlak liggen. We beginnen met de regulus $\mathcal{R}^+$:

$$b((\alpha,0,\beta,0),(0,\beta,0,\alpha)) = \alpha\beta + \beta\alpha = 2\alpha\beta.$$

Dit is enkel gelijk aan nul als $\alpha = 0$ of $\beta = 0$, want q is oneven. Aangezien α en β niet tegelijk nul mogen zijn, vinden we dat $\mathcal{R}^+$ twee absolute rechten bevat. Voor een rechte van de regulus $\mathcal{R}^-$, bekomen we

$$b((\alpha,0,0,\beta),(0,\beta,\alpha,0)) = \alpha\beta - \beta\alpha = 0.$$

Dit betekent dat alle $q+1$ rechten van $\mathcal{R}^-$ absoluut zijn. We hebben dus de beloofde strijdigheid gevonden omdat $q+1 = 1 \neq 2 \pmod p$. ■

Stel dat de verzameling $\mathcal{S}$ bestaat uit de absolute rechten van een symplectische polariteit $W(3,q)$. We definiëren de code $\mathcal{M}(3,q)$ als de code die wordt voortgebracht door de codewoorden van $\mathcal{M}_{1,1}(3,q)$ en de karakteristieke vectoren $\chi_\mathcal{S}$, met $\mathcal{S}$ variërend over alle symplectische polariteiten $W(3,q)$. Uit bovenstaande stelling volgt dat voor q even, $\mathcal{M}(3,q) = \mathcal{M}_{1,1}(3,q)$. Voor oneven q is $\mathcal{M}_{1,1}(3,q) \subset \mathcal{M}(3,q)$. We bewijzen eerst enkele eigenschappen voor $\mathcal{M}(3,q)$. Via deze eigenschappen zullen we de codewoorden met een klein gewicht van de code $\mathcal{M}(3,q)$ kunnen karakteriseren. Hieruit zal de karakterisering van de codewoorden met een klein gewicht van de code $\mathcal{M}_{1,1}(3,q)$ volgen.

Lemma 6.2.5. *[6, Lemma 4.5] Voor elk codewoord $c \in \mathcal{M}(3,q)$ bestaat er een getal $a \in \mathbb{F}_p$ zodat $c \cdot \chi_\mathcal{S} = a$ voor alle verzamelingen $\mathcal{S}$ uit de onderstaande lijst:*

- *$\mathcal{S}$ is de verzameling van alle rechten in $\mathrm{PG}(3,q)$,*
- *$\mathcal{S}$ is de verzameling van alle rechten door een punt in $\mathrm{PG}(3,q)$,*
- *$\mathcal{S}$ is de verzameling van alle rechten in een vlak van $\mathrm{PG}(3,q)$,*
- *$\mathcal{S}$ is de verzameling van alle rechten door een punt in een vlak van $\mathrm{PG}(3,q)$.*

Bewijs. De code $\mathcal{M}(3,q)$ wordt voortgebracht door de karakteristieke vectoren $\chi_l^{(1)}$ met l een rechte in $\mathrm{PG}(3,q)$ en de karakteristieke vector χ van een symplectische polariteit $W(3,q)$. We bewijzen dat voor deze vectoren de constante a uit de stelling gelijk is aan één. Merk op dat deze vectoren enkel coëfficiënten nul en één hebben. Ook de vector $\chi_\mathcal{S}$ met $\mathcal{S}$ zoals in het gegeven bevat enkel nullen en enen. Hierdoor is het bepalen van het inproduct equivalent met het tellen van het aantal gemeenschappelijke rechten in hun support. We bepalen hieronder $\chi_l^{(1)} \cdot \chi_\mathcal{S}$ en $\chi \cdot \chi_\mathcal{S}$ voor de verschillende vormen van $\mathcal{S}$.

- Geval 1: $\mathcal{S}$ is de verzameling van alle rechten in $\mathrm{PG}(3,q)$, m.a.w. $\chi_\mathcal{S} = \mathbf{1}$. Het gezochte inproduct $\chi_l^{(1)} \cdot \chi_\mathcal{S}$ en $\chi \cdot \chi_\mathcal{S}$ is dus respectievelijk gelijk aan $w(\chi_l^{(1)})$ en $w(\chi)$. We bepalen eerst $w(\chi_l^{(1)})$. Elk punt P van l ligt naast l op nog $\theta_2 - 1$ andere rechten. Omdat l juist $q+1$ punten bevat, vinden we $w(\chi_l^{(1)}) = 1 + (q+1)\cdot(\theta_2 - 1) = 1 \pmod p$. Daarnaast is het een gekend resultaat dat de symplectische polariteit $W(3,q)$ exact $(q+1)(q^2+1) = 1 \pmod p$ absolute rechten bevat.

- Geval 2: $\mathcal{S}$ is de verzameling van alle rechten door een punt P in $\mathrm{PG}(3,q)$. Voor het berekenen van $\chi_l^{(1)} \cdot \chi_\mathcal{S}$ zijn er twee mogelijkheden. Als $P \in l$, dan is $\mathrm{supp}(\chi_\mathcal{S}) \subseteq \mathrm{supp}(\chi_l^{(1)})$. Hieruit volgt dat $\chi_l^{(1)} \cdot \chi_\mathcal{S} = w(\chi_\mathcal{S}) = \theta_2 = 1 \pmod p$. Als $P \notin l$, dan zijn enkel de rechten door P die l snijden gemeenschappelijk in de support van $\chi_l^{(1)}$ en $\chi_\mathcal{S}$. Hierdoor is $\chi_l^{(1)} \cdot \chi_\mathcal{S} = q + 1 = 1 \pmod p$. Daarnaast is het aantal absolute rechten door een punt P van $W(3,q)$ gelijk aan $|W(1,q)| = q+1$. Dus is ook $\chi \cdot \chi_\mathcal{S} = 1$.

- Geval 3: $\mathcal{S}$ is de verzameling van alle rechten in een vlak π van $\mathrm{PG}(3,q)$. Voor het inproduct met $\chi_l^{(1)}$ splitsen we op in twee situaties. Als $l \subset \pi$, dan is $\mathrm{supp}(\chi_\mathcal{S}) \subseteq \mathrm{supp}(\chi_l^{(1)})$ omdat alle rechten in een vlak snijden. Zo vinden we dat $\chi_l^{(1)} \cdot \chi_\mathcal{S} = w(\chi_\mathcal{S}) = \theta_2 = 1 \pmod p$. Anders is de doorsnede van l en π een punt P. De enige gemeenschappelijke rechten in hun support zijn de rechten door P in π. Dit zijn er $q+1$, dus opnieuw is $\chi_l^{(1)} \cdot \chi_\mathcal{S} = 1 \pmod p$. Voor het inproduct met χ moeten we het aantal absolute rechten in het vlak π bepalen. Dit zijn alle rechten door het punt $\pi^\perp$ in π. Zo zijn er $q+1$, wat opnieuw $1 \pmod p$ geeft.

- Geval 4: $\mathcal{S}$ is de verzameling van alle rechten door een punt P in een vlak π van $\mathrm{PG}(3,q)$. Opnieuw splitsen we op in deelgevallen voor de rechte l: $l \subset \pi$ en $l \not\subset \pi$. In het eerste geval is $\mathrm{supp}(\chi_\mathcal{S}) \subseteq \mathrm{supp}(\chi_l^{(1)})$, en dus $\chi_l^{(1)} \cdot \chi_\mathcal{S} = w(\chi_\mathcal{S}) = q+1 = 1 \pmod p$. Anders snijdt l het vlak π in een punt Q. Als $Q = P$, dan is opnieuw $\mathrm{supp}(\chi_\mathcal{S}) \subseteq \mathrm{supp}(\chi_l^{(1)})$ en $\chi_l^{(1)} \cdot \chi_\mathcal{S} = 1 \pmod p$. Wanneer dit niet het geval is, hebben $\chi_\mathcal{S}$ en $\chi_l^{(1)}$ enkel de rechte $\langle P, Q\rangle$ gemeen in hun support. Dus is $\chi_l^{(1)} \cdot \chi_\mathcal{S} = 1$. Voor χ bespreken we ook twee deelgevallen. Als $P^\perp = \pi$, dan zijn alle rechten door P in π absoluut. Anders heeft het vlak π met $P^\perp$ juist één absolute rechte door P gemeen. Opnieuw is steeds $\chi \cdot \chi_\mathcal{S} = 1 \pmod p$.

Elk codewoord $c \in \mathcal{M}(3,q)$ is van de vorm $\sum_\chi a_\chi \chi + \sum_{l \in \mathrm{PG}(3,q)} a_l \chi_l^{(1)}$ waarbij de eerste som loopt over de karakteristieke vectoren van de absolute rechten van de symplectische polariteiten. Uit bovenstaande redenering volgt dat:

$$c \cdot \chi_\mathcal{S} = \sum_\chi a_\chi (\chi \cdot \chi_\mathcal{S}) + \sum_{l \in \mathrm{PG}(3,q)} a_l (\chi_l^{(1)} \cdot \chi_\mathcal{S}) = \sum_\chi a_\chi + \sum_{l \in \mathrm{PG}(3,q)} a_l.$$

Als we voor elk codewoord a kiezen als $\sum_\chi a_\chi + \sum_{l \in \mathrm{PG}(3,q)} a_l$, dan hebben we de stelling bewezen. ∎

Lemma 6.2.6. *[6, Lemma 4.7] Veronderstel dat $c \in \mathcal{M}(3,q)$ en dat $\mathcal{S}$ de verzameling is van ofwel alle rechten in een vlak π ofwel alle rechten door een punt P in $\mathrm{PG}(3,q)$. In het eerste geval behoort $c|_{\mathcal{S}}$ tot de code $\mathcal{M}_{1,0}(2,q)$ gedefinieerd in het vlak π. In het tweede geval is $c|_{\mathcal{S}}$ een codewoord van de code $\mathcal{C}_{0,1}(2,q) = \mathcal{M}_{0,1}(2,q)$ gedefinieerd in de quotiëntmeetkunde door het punt P.*

Bewijs. Stel dat c een codewoord is van $\mathcal{M}(3,q)$. Het idee is om te gebruiken dat c een lineaire combinatie is van vectoren van de vorm $\chi_l^{(1)}$, met l een rechte, en de karakteristieke vectoren χ horende bij de absolute rechten van één van de symplectische polariteiten $W(3,q)$. We tonen aan voor deze "basis" codewoorden de stelling juist is. Uit de lineariteit van de codes volgt het gevraagde.

Veronderstel eerst dat $\mathcal{S}$ de verzameling is van alle rechten door een punt P. We bewijzen dat $c|_{\mathcal{S}} \in \mathcal{C}_{0,1}(2,q)$ in de quotiëntmeetkunde door P voor $c \in \{\chi_l^{(1)}, \chi\}$. Als $P \in l$, dan is de beperking van $\chi_l^{(1)}$ tot $\mathcal{S}$ de vector $\mathbf{1}$. Als $P \notin l$, dan blijven enkel de rechten door P die l snijden behouden van $\chi_l^{(1)}$. Voor χ blijven enkel de absolute rechten door P behouden. In deze laatste twee mogelijkheden bekomen we dus telkens de karakteristieke vector van alle rechten door P in een vlak. In de quotiëntmeetkunde wordt dit de karakteristieke vector van alle punten in een rechte. Dit is duidelijk een codewoord van $\mathcal{C}_{0,1}(2,q)$. Ook het codewoord $\mathbf{1}$ vind je terug in deze code als de som van alle rijen van de incidentiematrix.

Stel nu dat $\mathcal{S}$ de verzameling is van alle rechten in het vlak π. Als $l \subset \pi$, dan is beperking van $\chi_l^{(1)}$ tot π de vector $\mathbf{1}$. Als $l \not\subset \pi$, dan is de beperking tot π de karakteristieke vector van alle rechten in π door het punt $\pi \cap l$. De beperking van de vector χ is ook de karakteristieke vector van alle rechten door een punt. Namelijk door het punt $\pi^\perp$. Dit zijn typische codewoorden uit de incidentiematrix van $\mathcal{M}_{1,0}(2,q)$. Het codewoord $\mathbf{1}$, kan men opnieuw bekomen door alle rijen van deze matrix op te tellen. ∎

We willen nu deze eigenschappen gebruiken om de karakterisering aan te tonen. Neem een codewoord $c \in \mathcal{M}(3,q)$ met $w(c) \leq q^3+2q^2+q+1$. We zullen aantonen dat de constante a uit Lemma 6.2.5 voor het codewoord c verschillend is van nul. Hiervoor gebruiken we dat we c kunnen beperken en zo een codewoord van $\mathcal{C}_{0,1}(2,q)$ of $\mathcal{M}_{1,0}(2,q)$ vinden. Szőnyi en Weiner hebben bewezen hoe de codewoorden met een voldoende klein gewicht in de code $\mathcal{C}_{0,1}(2,q)$ eruit zien. Dit staat beschreven in onderstaande stelling en we aanvaarden dit resultaat zonder bewijs. Via de dualiteit van het projectieve vlak volgt hieruit wat de codewoorden met hetzelfde gewicht van $\mathcal{M}_{1,0}(2,q)$ zijn. De stelling daarna, Stelling 6.2.8, is de laatste tussenstap voor we de codewoorden c met $a = 0$ uitsluiten. We bewijzen eerst Stelling 6.2.8 zoals Stinson.

Stelling 6.2.7. *[40] Gegeven een codewoord c van de code $\mathcal{C}_{0,1}(2,q)$, met $q \geq 19$. Als $w(c)$ kleiner is dan $3q-3$ voor q priem of kleiner dan $3q-12$ als q niet priem is, dan is c de lineaire combinatie van hoogstens twee karakteristieke vectoren van rechten.*

Stelling 6.2.8. *[37] Een verzameling rechten $\mathcal{S}$ in $\mathrm{PG}(2,q)$ bedekt minstens $\frac{(q+1)^2|\mathcal{S}|}{q+|\mathcal{S}|}$ punten.*

Bewijs. We zullen deze stelling bewijzen door de dualiteit van het projectieve vlak te gebruiken. Stel dat $\mathcal{S}$ een verzameling punten in $\mathrm{PG}(2,q)$ is. De verzameling $\mathcal{V}$ bestaat uit de rechten die minstens één punt van $\mathcal{S}$ bevatten. We bewijzen dat het aantal bedekte rechten door $\mathcal{S}$, i.e. $|\mathcal{V}|$, minstens $\frac{(q+1)^2|\mathcal{S}|}{q+|\mathcal{S}|}$ is. We doen dit zoals in het bewijs van [37, Theorem 3.1]. Via de dualiteit van het projectieve vlak volgt dan dat de stelling waar is. Neem een rechte l van $\mathcal{V}$. De verzameling $l_{\mathcal{S}}$ bestaat uit de punten van de rechte l die ook in de verzameling $\mathcal{S}$ liggen. We definiëren de verzameling $\mathcal{B}$ als de verzameling $\{l_{\mathcal{S}} \mid l \in \mathcal{V}\}$. Het is duidelijk dat $|\mathcal{V}| = |\mathcal{B}|$. We bekijken nu de incidentie structuur $(\mathcal{S}, \mathcal{B})$. We tellen de koppels $(P, l_{\mathcal{S}})$, met $(P, l_{\mathcal{S}}) \in (\mathcal{S}, \mathcal{B})$ en $P \in l_{\mathcal{S}}$, op

twee manieren. Elk punt van $\mathcal{S}$ ligt in $q+1$ rechten. Al deze $q+1$ rechten behoren tot $\mathcal{V}$ en geven zo aanleiding tot $q+1$ blokken van $\mathcal{B}$. Dus elk punt van $\mathcal{S}$ ligt in $q+1$ blokken. Het aantal koppels is bijgevolg $(q+1)|\mathcal{S}|$. We kunnen dit aantal ook bepalen door het aantal punten in elk blok $l_\mathcal{S}$ op te tellen. Zo vinden we de gelijkheid die hieronder staat. We bespreken nu hoe we aan de gelijkheid daarnaast komen. We tellen hiervoor het totale aantal blokken door alle puntenparen op twee manieren. Elk paar punten van $\mathcal{S}$ ligt in juist één rechte l en dus in juist één blok $l_\mathcal{S}$. Hieruit volgt dat het gezochte aantal $\binom{|\mathcal{S}|}{2}$ is. Langs de andere kant kunnen we ook in elk blok het aantal puntenparen tellen. Zo vinden we de volgende gelijkheden:

$$\sum_{l_\mathcal{S}\in\mathcal{B}} |l_\mathcal{S}| = (q+1)|\mathcal{S}| \text{ en } \sum_{l_\mathcal{S}\in\mathcal{B}} \binom{|l_\mathcal{S}|}{2} = \binom{|\mathcal{S}|}{2}.$$

Wanneer we de eerste vergelijking optellen bij tweemaal de tweede vergelijking, vinden we:

$$\sum_{l_\mathcal{S}\in\mathcal{B}} |l_\mathcal{S}|^2 = (q+|\mathcal{S}|)|\mathcal{S}|.$$

We bepalen nu het gemiddelde aantal punten b dat een blok $l_\mathcal{S}$ door een vast punt P bevat. Het punt P van $\mathcal{S}$ ligt op $q+1$ blokken. Alle punten van $\mathcal{S}\setminus\{P\}$ liggen op juist één zo'n blok. Het punt P zelf ligt natuurlijk ook op elk van de $q+1$ blokken. Zo vinden dat een blok door een punt P gemiddeld $b = \frac{(|\mathcal{S}|-1)+(q+1)}{q+1} = \frac{|\mathcal{S}|+q}{q+1}$ punten bevat. We bekijken de afwijking die hierop te vinden is en passen de gevonden gelijkheden hierin toe:

$$\begin{aligned}
&0 \le \sum_{l_\mathcal{S}\in\mathcal{B}} (|l_\mathcal{S}|-b)^2 = \sum_{l_\mathcal{S}\in\mathcal{B}} |l_\mathcal{S}|^2 - 2b\sum_{l_\mathcal{S}\in\mathcal{B}} |l_\mathcal{S}| + \sum_{l_\mathcal{S}\in\mathcal{B}} b^2 \\
\iff &0 \le (q+|\mathcal{S}|)|\mathcal{S}| - 2b(q+1)|\mathcal{S}| + b^2|\mathcal{B}| \\
\iff &0 \le (q+|\mathcal{S}|)|\mathcal{S}| - 2(q+1)|\mathcal{S}|\left(\frac{|\mathcal{S}|+q}{q+1}\right) + |\mathcal{B}|\left(\frac{|\mathcal{S}|+q}{q+1}\right)^2 \\
\iff &2|\mathcal{S}|(|\mathcal{S}|+q) - (q+|\mathcal{S}|)|\mathcal{S}| \le |\mathcal{B}|\left(\frac{|\mathcal{S}|+q}{q+1}\right)^2 \\
\iff &|\mathcal{S}|(|\mathcal{S}|+q) \le |\mathcal{B}|\left(\frac{|\mathcal{S}|+q}{q+1}\right)^2 \\
\iff &\frac{(q+1)^2|\mathcal{S}|}{|\mathcal{S}|+q} \le |\mathcal{B}|.
\end{aligned}$$

Omdat $|\mathcal{B}| = |\mathcal{V}|$ hebben we de gewenste ondergrens gevonden. ■

We bewijzen nu de beloofde stelling over de codewoorden $c \in \mathcal{M}(3,q)$ met $a = 0$.

Stelling 6.2.9. *[6, Proposition 4.8] Veronderstel dat $c \in \mathcal{M}(3,q)$, met $q \ge 19$, en $c\cdot\mathbf{1} = 0$. Als c niet de nulvector is, dan is $w(c) \ge q^3+2q^2+q+3$.*

Bewijs. Neem een codewoord $c \in \mathcal{M}(3,q)$ verschillend van de nulvector zodat $c\cdot\mathbf{1} = 0$. De verzameling rechten die $\mathrm{supp}(c)$ vormt, noteren we kort als $\mathcal{S}$. We definiëren δ als 3 wanneer q een priemgetal is en als 12 anders. Dit is zodat we later makkelijk Stelling 6.2.7 zouden kunnen toepassen. We bewijzen eerst dat elk punt op 0, $2q$ of minstens $3q-\delta$ rechten van $\mathcal{S}$ ligt. Nadien tonen we analoog aan dat elk vlak 0, $2q$ of minstens $3q-\delta$ rechten bevat van $\mathcal{S}$. Beschouw een punt P dat op minstens één rechte van $\mathcal{S}$ ligt. De verzameling van alle rechten door P noteren we als de verzameling $\mathcal{V}$. Dankzij Stelling 6.2.6 weten we dat $c|_\mathcal{V} \in \mathcal{C}_{0,1}(2,q)$. Veronderstel dat er minder dan $3q-\delta$ rechten van $\mathcal{S}$ bevat zijn in $\mathcal{V}$. We willen dan bewijzen dat $|\mathcal{V}| = 2q$. Uit Stelling 6.2.7 volgt

dat $c|_{\mathcal{V}}$ een lineaire combinatie is van hoogstens twee incidentievectoren van rechten l en m in de quotiëntmeetkunde door P. Met andere woorden $c|_{\mathcal{V}} = a\chi_l^{(0)} + b\chi_m^{(0)}$ voor $a, b \in \mathbb{F}_p$. Via Lemma 6.2.5 volgt dat $c \cdot \chi_{\mathcal{V}} = c \cdot \mathbf{1}$, want $\mathbf{1}$ is de karakteristieke vector van de verzameling bestaande uit alle rechten in $\mathrm{PG}(3, q)$. We vinden dus dat $a + b = c|_{\mathcal{V}} \cdot \mathbf{1} = c \cdot \chi_{\mathcal{V}} = c \cdot \mathbf{1} = 0$. Bijgevolg is $a = -b$. Omdat minstens één rechte door P bevat is in $\mathcal{S}$, is $c|_{\mathcal{V}} = a\chi_l^{(0)} + b\chi_m^{(0)} \neq \mathbf{0}$. Daardoor is $l \neq m$ en $a = -b \neq 0$. Hieruit leiden we af dat de support van $c|_{\mathcal{V}}$ bestaat uit alle punten van de rechten l en m behalve hun snijpunt. Wanneer we terugkeren van de quotiëntmeetkunde door P naar $\mathrm{PG}(3, q)$ vertaalt dit zich naar het feit dat er juist $2q$ rechten door P behoren tot $\mathcal{S}$. Deze $2q$ rechten liggen in twee verschillende vlakken. Beide vlakken bevatten juist q rechten door P van $\mathcal{S}$. De ontbrekende rechte door P in elk vlak is de snijlijn van de twee vlakken. We besluiten dat een verzameling $\mathcal{V}$ bestaande uit rechten van $\mathcal{S}$ door een willekeurig punt P, met $0 < |\mathcal{V}| < 3q - \delta$, bestaat uit juist $2q$ rechten door P.

Analoog tonen we aan dat elk vlak 0, $2q$ of $3q-\delta$ rechten bevat van $\mathcal{S}$. Stel dat π minstens één, maar minder dan $3q-\delta$ rechten bevat van $\mathcal{S}$. De verzameling van rechten van $\mathcal{S}$ in het vlak π noteren we als $\mathcal{V}$. Uit Stelling 6.2.6 weten we dat $c|_{\mathcal{V}} \in \mathcal{C}_{1,0}(2, q)$. Omdat $w(c) < 3q - \delta$ en dankzij de dualiteit in het projectieve vlak kunnen we Stelling 6.2.7 gebruiken. Zo vinden we dat $c|_{\mathcal{V}} = a\chi_Q^{(1)} + b\chi_R^{(1)}$, met Q en R punten in π en $a, b \in \mathbb{F}_p$. Zoals voordien volgt er via Lemma 6.2.5 en het gegeven dat $a = -b$. Aangezien er minstens één rechte van $\mathcal{S}$ bevat is in π, bekomen we dat $a\chi_Q^{(1)} + b\chi_R^{(1)} \neq \mathbf{0}$. Hieruit besluiten we dat $Q \neq R$ en $a = -b \neq 0$. Er zijn dus juist $2q$ rechten van $\mathcal{S}$ die in π liggen. Deze gaan ofwel door het punt Q ofwel door het punt R, maar niet door beide.

We bewijzen vervolgens de stelling als er een punt P bestaat zodat juist $2q$ rechten door P behoren tot $\mathcal{S}$. Daarna bespreken we dat de stelling voldaan is als er een vlak bestaat waar exact $2q$ rechten van $\mathcal{S}$ in liggen. Stel dat er juist $2q$ rechten door het punt P behoren tot $\mathcal{S}$. We weten dat er dan twee vlakken π en π' bestaan door P die elk q van deze rechten bevatten. Ook is de rechte $\pi \cap \pi'$ geen element van $\mathcal{S}$. We tellen het aantal rechten in de verzameling $\mathcal{S}$ via de vlakken door het punt P. De vlakken π en π' leveren samen al een bijdrage van $2q$ rechten. De andere vlakken door P die niet de rechte $\pi \cap \pi'$ bevatten, snijden π en π' in een rechte van $\mathcal{S}$. Deze moeten dus nog minstens $2q - 2$ extra rechten bevatten. Er zijn θ_2 vlakken door het punt P, waarvan er θ_1 gaan door $\pi \cap \pi'$. Zo vinden we q^2 vlakken die elk minstens $2q - 2$ extra rechten van $\mathcal{S}$ bevatten. We bekomen zo de volgende ondergrens voor $w(c)$:

$$w(c) \geq 2 \cdot 2q + q^2 \cdot (2q - 2) = 2q^3 - 2q^2 + 4q.$$

Dit is groter dan het gewicht uit de stelling dat we willen als ondergrens:

$$2q^3 - 2q^2 + 4q > q^3 + 2q^2 + q + 3 \iff q^3 - 4q^2 + 3q - 3 > 0.$$

Men kan controleren dat dit polynoom inderdaad positief is voor $q \geq 1$. Als er een vlak π met daarin $2q$ rechten van $\mathcal{S}$ bestaat, kunnen we dezelfde ondergrens aantonen. Dit kan men doen door alle rechten van $\mathcal{S}$ door het punt Q, het punt R en de punten uit de verzameling $\pi \setminus \langle Q, R \rangle$ te tellen. Hierin zijn de punten Q en R zoals hierboven gedefinieerd. De details laten we over als oefening voor de lezer.

Vanaf nu kunnen we er dus vanuit gaan dat geen enkel punt of vlak incident is met precies $2q$ rechten van $\mathcal{S}$. We bewijzen dat ook dan de stelling geldt. Beschouw een vlak π dat minstens één rechte van $\mathcal{S}$ bevat. Er volgt dan dat π minstens $3q - \delta$ rechten van $\mathcal{S}$ bevat. Uit Stelling 6.2.8 weten we dat al deze rechten samen minstens $\frac{(q+1)^2(3q-\delta)}{4q-\delta}$ verschillende punten bevatten van π. Elk zo'n punt P ligt op minstens $3q - \delta$ rechten van $\mathcal{S}$. Maar hoogstens $q + 1$ rechten door P liggen in het vlak π. Hieruit volgt dat elk van deze $\frac{(q+1)^2(3q-\delta)}{4q-\delta}$ punten P op minstens $2q - \delta - 1$

verschillende rechten buiten π ligt. We gebruiken dit om opnieuw een minimum te bepalen voor het aantal rechten van $\mathcal{S}$:

$$w(c) \geq 3q - \delta + (2q - 1 - \delta)\frac{(q+1)^2(3q-\delta)}{4q-\delta}.$$

We hebben δ gedefinieerd als 3 voor $q = p$ priem en als 12 voor $q = p^h$ met $h > 1$. Dankzij het gegeven is $q \geq 19$. Dit betekent dat de drie eerstvolgende mogelijkheden voor q de getallen 19, 23 en 25 zijn. Deze eerste twee zijn priemgetallen en voor hen bekijken we de waarde $\delta = 3$. Voor 25 bekijken we $\delta = 12$. Voor deze combinaties zien we dat $w(c) \geq q^3 + 2q^2 + q + 3$. Via de computer kan men nagaan dat ook voor grotere q onze gevonden ondergrens groter is dan $q^3 + 2q^2 + q + 3$. Dus is de stelling bewezen. ■

Om de karakterisering van de codewoorden met een klein gewicht van $\mathcal{M}(3, q)$ te vervolledigen hebben we ook een resultaat over blokkerende verzamelingen nodig. Meer bepaald aanvaarden we onderstaand resultaat over een minimale blokkerende verzameling $\mathcal{B}$ t.o.v. de rechten van een hyperbolische kwadriek $Q^+(5, q)$. Dankzij de Klein correspondentie is een codewoord $c \in \mathcal{M}(3, q)$ waarvoor de constante a uit Stelling 6.2.5 niet nul is, equivalent met zo'n verzameling $\mathcal{B}$. De details hiervan leggen we uit in onderstaand bewijs van de karakterisering.

Stelling 6.2.10. *[6, Theorem 1.4] Stel dat $\mathcal{B}$ een minimale blokkerende verzameling is voor de rechten van $Q^+(5, q)$, met $q \geq 4$. Als $|\mathcal{B}| \leq q^3 + 2q^2 + q + 1$, dan liggen alle punten van $\mathcal{B}$ in de doorsnede van een hypervlak met $Q^+(5, q)$.*

Stelling 6.2.11. *[6, Theorem 4.9] Beschouw een niet-nul codewoord c van $\mathcal{M}(3, q)$ met $w(c) \leq q^3 + 2q^2 + q + 1$, voor $q \geq 19$. Het codewoord c heeft dan één van de volgende vormen:*

- $w(c) = q^3 + q^2 + q + 1$ *en c is het scalair veelvoud van de karakteristieke vector van de verzameling rechten van een symplectische polariteit $W(3, q)$.*
- $w(c) = q^3 + 2q^2 + q + 1$ *en c is het scalair veelvoud van de karakteristieke vector $\chi_l^{(1)}$ van een rechte l.*

Bewijs. Neem een codewoord c van de code $\mathcal{M}(3, q)$ zodat $w(c) \leq q^3 + 2q + q + 1$. Uit Stelling 6.2.9 volgt dat $c \cdot \mathbf{1} = a \neq 0$. We kunnen nu Stelling 6.2.5 uitbuiten om aan te tonen dat $\mathrm{supp}(c)$ overeenkomt met een blokkerende verzameling van de rechten van een hyperbolische kwadriek $Q^+(5, q)$. Via de Klein correspondentie weten we dat elke rechte l van $Q^+(5, q)$ overeenkomt met een vlakke stralenwaaier $\mathcal{L}$ in $\mathrm{PG}(3, q)$. Dankzij Stelling 6.2.5 weten we dat $\mathrm{supp}(c)$ minstens één rechte l' gemeen heeft met $\mathcal{L}$, want $a \neq 0$. De rechte l' correspondeert met een punt op de rechte l van $Q^+(5, q)$. Omdat l willekeurig gekozen is, volgt dat $\mathrm{supp}(c)$ equivalent is met een blokkerende verzameling $\mathcal{B}$ t.o.v. de rechten van $Q^+(5, q)$. De verzameling $\mathcal{B}$ bevat een minimale blokkerende verzameling $\mathcal{B}'$. We mogen Stelling 6.2.10 toepassen op $\mathcal{B}'$, want

$$|\mathcal{B}'| \leq |\mathcal{B}| = |\mathrm{supp}(c)| \leq q^3 + 2q^2 + q + 1.$$

Dit betekent dat $\mathcal{B}'$ bevat is in de doorsnede van een hypervlak π met $Q^+(5, q)$. Dit geeft twee mogelijkheden.

Geval 1: $\pi \cap Q^+(5, q) = Q(4, q)$. In dit geval moet $\mathcal{B}'$ bestaan uit alle punten van $Q(4, q)$. Inderdaad stel dat $\mathcal{B}'$ een punt $P \in Q(4, q)$ niet bevat. De rechten door P van $Q^+(5, q)$ spannen het raakhypervlak van P op. Aangezien dit van de vorm $PQ^+(3, q)$ is, is dit verschillend van π. Bijgevolg vinden we een rechte m door P die niet in π ligt, maar wel een deel is van de kwadriek $Q^+(5, q)$. Er ligt echter geen punt van $\mathcal{B}'$ in de rechte m wat een strijdigheid geeft. We besluiten dat

$\mathcal{B}' = Q(4,q)$. Via de Klein correspondentie weten we dat de punten van deze $Q(4,q)$ overeenkomen met de rechten van een symplectische polariteit $W(3,q)$. Als we de verzameling van absolute rechten van $W(3,q)$ noteren met $\mathcal{S}$, vinden we $\mathcal{S} \subseteq \text{supp}(c)$. We kiezen c' als het codewoord $a\chi_{\mathcal{S}}$, dan is ook $\text{supp}(c') \subseteq \text{supp}(c)$. Hieruit volgt dat $w(c-c') \leq w(c')$.

Geval 2: $\pi \cap Q^+(5,q) = PQ^+(3,q)$. Via dezelfde redenering als hierboven zien we dat $\mathcal{B}'$ bestaat uit de punten van $PQ^+(3,q)$ behalve het punt P. Opnieuw via de Klein correspondentie komt dit overeen met een verzameling rechten $\mathcal{S}$ in $\text{PG}(3,q)$. Deze verzameling bestaat uit alle rechten in $\text{PG}(3,q)$ die een rechte m snijden in juist één punt. Hierbij correspondeert m met het punt P. Bekijk het codewoord $\chi_m^{(1)} \in \mathcal{M}(3,q)$. Er geldt dat de support van $\chi_m^{(1)}$ zonder de rechte m een deel is van $\text{supp}(c)$. Merk op dat we op dit moment niet weten of de rechte m ook een deel is van $\text{supp}(c)$. Vervolgens definiëren we het codewoord c' als $a\chi_m^{(1)}$. We vinden dat $w(c-c') \leq w(c)+1$. Het is noodzakelijk om hierin het gewicht van c met één te verhogen voor het geval dat de rechte m niet zou behoren tot $\text{supp}(c)$.

We vinden dus telkens een codewoord $c-c'$ zodat $w(c-c') \leq w(c)+1 < q^3+2q^2+q+3$. Ook is $(c-c')\cdot\mathbf{1} = c\cdot\mathbf{1} - c'\cdot\mathbf{1} = a - aw(c') = a - a = 0 \pmod p$. Hierbij gebruikten we dat $w(c')$ in beide gevallen gelijk is aan $1 \pmod p$, omdat $w(\chi_m^{(1)}) = 1+(q+1)(\theta_2-1) = q^3+2q^2+q+1$ en $w(\chi_{\mathcal{S}}) = (q+1)(q^2+1) = q^3+q^2+q+1$ zoals we in het bewijs van Stelling 6.2.5 berekenden. Uit Stelling 6.2.9 volgt dat $c-c'$ de nulvector moet zijn, zodat $c = c'$. Omdat de twee mogelijkheden voor c' overeenkomen met de vormen uit het te bewijzen, hebben we de stelling bewezen. ■

We leiden nu hieruit de beloofde karakterisering van de codewoorden met een klein gewicht van $\mathcal{M}_{1,1}(3,q)$ af. Merk op dat in het bijzonder het minimum gewicht van $\mathcal{M}_{1,1}(3,q)$ groter is voor oneven q.

Stelling 6.2.12. *[6, Theorem 1.2] Beschouw een niet-nul codewoord c van $\mathcal{M}_{1,1}(3,q)$ met $w(c) \leq q^3+2q^2+q+1$, voor $q \geq 19$. Het codewoord c voldoet dan één van de volgende vormen:*

- $w(c) = q^3+q^2+q+1$ *en c is het scalair veelvoud van de karakteristieke vector van de verzameling rechten van een symplectische polariteit $W(3,q)$. Dit geval treedt enkel op als en slechts als q even is.*
- $w(c) = q^3+2q^2+q+1$ *en c is het scalair veelvoud van de karakteristieke vector $\chi_l^{(1)}$ van een rechte l.*

Bewijs. De code $\mathcal{M}_{1,1}(3,q)$ is bevat in de code $\mathcal{M}(3,q)$. Uit Stelling 6.2.11 volgt dat een codewoord $c \in \mathcal{M}_{1,1}(3,q)$ met $w(c) \leq q^3+2q^2+q+1$ één van de vormen heeft uit de stelling. Dankzij Stelling 6.2.4 weten we dat het eerste geval enkel kan optreden als en slechts als q even is. Dit is wat we wilden bewijzen. ■

Om te eindigen merken we op dat er een verband is tussen de codes $\mathcal{M}_{1,1}(3,q)$ en $\mathcal{C}_{1,2}(3,q)$. Het bewijs dat we hieronder bespreken is gegeven aan de auteur door Sam Adriaensen. Mogelijk zijn er nog meer verbanden tussen de codes $\mathcal{M}_{j,k}(n,q)$ en $\mathcal{C}_{j,k'}(n,q)$, dit vereist verder onderzoek.

Stelling 6.2.13. *De code $\mathcal{M}_{1,1}(3,q)$ is een deelcode van $\mathcal{C}_{1,2}(3,q)$.*

Bewijs. De code $\mathcal{C}_{1,2}(3,q)$ wordt voortgebracht door de karakteristieke vectoren χ_π horende bij de vlakken π in $\text{PG}(3,q)$. De vector χ_π duidt aan welke rechten liggen in π. Neem een willekeurige rechte l in $\text{PG}(3,q)$. Als de bijhorende karakteristieke vector $\chi_l^{(1)}$ behoort tot $\mathcal{C}_{1,2}(3,q)$, dan zal $\mathcal{M}_{1,1}(3,q) \subseteq \mathcal{C}_{1,2}(3,q)$. We tonen aan dat dit inderdaad het geval is. Beschouw de $q+1$ verschillende vlakken π_i door de rechte l, met $i \in \{1,\ldots,q+1\}$. Het codewoord $c = \chi_{\pi_1} + \cdots + \chi_{\pi_{q+1}}$ behoort tot $\mathcal{C}_{1,2}(3,q)$. Ook is de coëfficiënt van de rechte l hierin gelijk aan $q+1 = 1 \pmod p$.

Daarnaast ligt elke rechte die l snijdt in exact één vlak π_i. De bijhorende coëfficiënt in c is dus één. De rechten die l niet snijden, liggen in geen enkel vlak π_i dus deze hebben coëfficiënt nul in c. We mogen dus besluiten dat $c = \chi_l^{(1)}$. ■

6.3. Code van klassieke polaire ruimten

In de code $\mathcal{C}_k(n, q)$ bekijken we in onze incidentiematrix alle k-ruimten. We zouden ook enkel de k-ruimten kunnen toelaten die bevat zijn in een bepaalde structuur zoals een kwadriek. Stel dat $\mathcal{P}$ een klassieke polaire ruimte is die k-ruimten bevat en $\mathrm{PG}(n, q)$ voortbrengt. We noteren de beperking tot de k-ruimten van $\mathcal{P}$ als de code $\mathcal{C}_k(\mathcal{P})$. Het is duidelijk dat $\mathcal{C}_k(\mathcal{P}) \subseteq \mathcal{C}_k(n, q)$. Zoals opgemerkt door Pepe, Storme en Van de Voorde in [31] kunnen we dus de classificatie resultaten voor codewoorden met een klein gewicht van $\mathcal{C}_k(n, q)$ gebruiken voor $\mathcal{C}_k(\mathcal{P})$. Het enige dat men moet controleren is of het codewoord van $\mathcal{C}_k(n, q)$ ook voorkomt in $\mathcal{C}_k(\mathcal{P})$. Zo vinden we dat de minimum gewicht codewoorden van $\mathcal{C}_k(\mathcal{P})$ scalaire veelvouden zijn van k-ruimten bevat in de polaire ruimte $\mathcal{P}$. Analoog zouden we de code $\mathcal{C}_{j,k}(n, q)$ kunnen beperken tot de k-ruimten in de kwadriek $\mathcal{P}$. Zo bekomen we de code $\mathcal{C}_{j,k}(\mathcal{P}) \subseteq \mathcal{C}_{j,k}(n, q)$.

Voor de duale code mogen we geen resultaten overnemen. Inderdaad, uit $\mathcal{C}_k(\mathcal{P}) \subseteq \mathcal{C}_k(n, q)$ volgt dat $\mathcal{C}_k(n, q)^\perp \subseteq \mathcal{C}_k(\mathcal{P})^\perp$. In [31] bekijken Pepe, Storme en Van de Voorde codewoorden met een klein of groot gewicht voor specifieke polaire ruimten $\mathcal{P}$. Ter illustratie bespreken we hieronder kort één van deze resultaten, voor verdere informatie verwijzen we naar [31]. Een ander interessant artikel voor de geïnteresseerde lezer is [15] van Vandendriessche en De Boeck waarin ze verdere classificatie resultaten voor de Hermitische variëteit $\mathcal{H}(2n + 1, q^2)$ bewijzen.

Veronderstel dat $\mathcal{P}$ de hyperbolische kwadriek $Q^+(5, q)$ is. De codewoorden van $\mathcal{C}_2(Q^+(5, q))^\perp$ met gewicht hoogstens $4q + 4$ voor $q > 124$ zijn door Pepe, Storme en Van de Voorde in [31] gekarakteriseerd. De uitleg hieronder over hoe deze codewoorden geconstrueerd worden is gebaseerd op dit artikel. Stel dat c een codewoord is van $\mathcal{C}_2(Q^+(5, q))^\perp$. We noteren $\mathrm{supp}(c)$ als $\mathcal{S}$. Elk vlak π van $Q^+(5, q)$ bevat nul of minstens twee punten van $\mathcal{S}$. Via de Klein correspondentie is er een bijectie tussen $\mathcal{S}$ en een verzameling rechten $\mathcal{L}_\mathcal{S}$ in $\mathrm{PG}(3, q)$. Het vlak π komt overeen met alle rechten in een vlak of alle rechten door een punt in $\mathrm{PG}(3, q)$. Zo geldt er voor elk vlak en elk punt in $\mathrm{PG}(3, q)$ dat het incident is met nul of minstens twee rechten van $\mathcal{L}_\mathcal{S}$. Daarnaast is de som van de coëfficiënten die horen bij de incidente rechten van $\mathcal{L}_\mathcal{S}$ met een vast punt of een vast vlak gelijk aan nul, opdat $(c, \pi) = 0$. Als we een verzameling $\mathcal{L}_\mathcal{S}$ en bijhorende coëfficiënten kiezen die hieraan voldoen, vinden we een codewoord van $\mathcal{C}_2(Q^+(5, q))^\perp$. We kunnen nu op deze manier twee voorbeelden construeren.

Voorbeeld 6.3.1. [31, Example 23] We kiezen $\mathcal{L}_\mathcal{S}$ als de $2q + 2$ rechten van een hyperbolische kwadriek $Q^+(3, q)$ in $\mathrm{PG}(3, q)$. Stel dat de reguli van $Q^+(3, q)$ de verzamelingen $\mathcal{R}^+$ en $\mathcal{R}^-$ zijn, dan is $\mathcal{L}_\mathcal{S} = \{\mathcal{R}^+, \mathcal{R}^-\}$. De rechten van $\mathcal{R}^+$ geven we coëfficiënt a, met $a \in \mathbb{F}_q^*$. De rechten van $\mathcal{R}^-$ krijgen coëfficiënt $-a$. We controleren dat $\mathcal{L}_\mathcal{S}$ aan de voorwaarden voldoet. Als een punt P op een rechte van de kwadriek ligt, dan ligt P op juist één rechte van beide reguli. Door de gekozen coëfficiënten is de som van alle rechten van $\mathcal{L}_\mathcal{S}$ door P gelijk aan nul. De voorwaarden voor de punten is dus in orde. We controleren nu de vlakken. In een vlak π liggen er enkel rechten van $Q^+(3, q)$ als π een raakvlak is. Een raakvlak bevat één rechte van elke reguli. De som van de coëfficiënten van deze rechten is ook opnieuw nul. Dus voldoet $\mathcal{L}_\mathcal{S}$ aan alle voorwaarden om een codewoord van $\mathcal{C}_2(Q^+(5, q))^\perp$ te zijn. Via de Klein correspondentie is de bijhorende verzameling $\mathcal{S}$ gelijk aan twee kegelsneden in twee scheve vlakken van $\mathrm{PG}(5, q)$. Bovendien zijn deze twee vlakken elkaars beeld onder de polariteit en zijn beide vlakken niet bevat in $Q^+(5, q)$.

Voorbeeld 6.3.2. [31, Example 24] Kies twee verschillende punten P en R en twee vlakken π_1 en π_2 door de rechte $\langle P, R\rangle$ in $\mathrm{PG}(3, q)$. We kiezen $\mathcal{L}_\mathcal{S}$ als de verzameling rechten door het punt P of R en in het vlak π_1 of π_2, maar verschillend van de rechte $\langle P, R\rangle$. Dan is $|\mathcal{L}_\mathcal{S}| = 4q$. Alle rechten door P in π_1 en door R in π_2 krijgen coëfficiënt a, met $a \in \mathbb{F}_q^*$. De andere rechten van $\mathcal{L}_\mathcal{S}$ geven we coëfficiënt $-a$. Zo zien we onmiddellijk dat de punten P en R en de vlakken π_1 en π_2 voldoen aan de voorwaarden. Een punt dat niet in π_1 of π_2 ligt of een punt op $\langle P, R\rangle \setminus \{P, R\}$, ligt op geen enkele rechte van $\mathcal{L}_\mathcal{S}$. Een punt Q verschillend van P en R dat wel in één van deze vlakken ligt, ligt op twee rechten van $\mathcal{L}_\mathcal{S}$: $\langle Q, P\rangle$ en $\langle Q, R\rangle$. Omdat deze verschillende coëfficiënten hebben, is de voorwaarde voor de punten voldaan. In $\mathrm{PG}(3, q)$ hebben alle vlakken minstens een rechte gemeen. Neem een vlak π verschillend van π_1 en π_2. Stel dat π het vlak π_1 snijdt in een rechte door P. Dan snijdt π ook π_2 in een rechte door P. Als dit de rechte $\langle P, R\rangle$ is, bevat π geen rechten van $\mathcal{L}_\mathcal{S}$. Anders bevat π juist twee rechten met tegenovergestelde coëfficiënt van $\mathcal{L}_\mathcal{S}$. Analoog zien we dat de voorwaarde voldaan is wanneer het vlak π het vlak π_1 snijdt in een rechte door R. Het laatste geval is dat π het vlak π_1 snijdt in een rechte die P en R niet bevat. Er liggen dan geen rechten van $\mathcal{L}_\mathcal{S}$ in π. Zo zien we dat $\mathcal{L}_\mathcal{S}$ voldoet aan de voorwaarden. We kunnen ons nu afvragen hoe de corresponderende verzameling $\mathcal{S}$ eruit ziet. Dit zijn $4q$ punten zijn die op vier rechten door een punt $T \in Q^+(5, q)$ liggen. Hierbij komt het punt T overeen met de rechte $\langle P, R\rangle$ en is T geen deel van de verzameling $\mathcal{S}$. Deze rechten definiëren een vierhoek op de basis van de raakkegel $TQ^+(3, q)$.

Ten slotte geven we hieronder zonder bewijs de karakterisering van de codewoorden met gewicht hoogstens $4q + 4$ van $\mathcal{C}_2(Q^+(5, q))^\perp$ als $q > 124$. De codewoorden met minimum gewicht zijn deze uit het eerste voorbeeld. Hiermee hebben we dit laatste deel afgewerkt.

Stelling 6.3.3. *[31, Theorem 32] Beschouw een niet-nul codewoord c van de code $\mathcal{C}_2(Q^+(5, q))^\perp$, met $q > 124$. Via de Klein correspondentie komt $\mathrm{supp}(c)$ overeen met een verzameling rechten $\mathcal{L}_\mathcal{S}$ in $\mathrm{PG}(3, q)$. Als het gewicht van c hoogstens $4q + 4$ is, dan hebben de verzameling $\mathcal{L}_\mathcal{S}$ en de bijhorende coëfficiënten één van volgende vormen:*

- *$\mathcal{L}_\mathcal{S}$ bestaat uit alle rechten van een hyperbolische kwadriek $Q^+(3, q)$. De rechten in één regulus krijgen coëfficiënt $a \in \mathbb{F}_q^*$, de rechten uit de tegenovergestelde regulus hebben coëfficiënt $-a$.*
- *$\mathcal{L}_\mathcal{S}$ en de coëfficiënten zijn een lineaire combinatie van twee codewoorden zoals in bovenstaand puntje. Rechten die een coëfficiënt nul krijgen door deze lineaire combinatie, behoren niet tot $\mathcal{L}_\mathcal{S}$.*
- *$\mathcal{L}_\mathcal{S}$ bestaat uit de rechten door één van de twee punten P en R die in twee vlakken π_1 en π_2 door $\langle P, R\rangle$ liggen, behalve de rechte $\langle P, R\rangle$. De rechten door P in π_1 en door R in π_2 krijgen coëfficiënt a, met $a \in \mathbb{F}_q^*$, de andere rechten hebben coëfficiënt $-a$.*

7 Besluit

Om te eindigen geven we een overzicht van de besproken resultaten. In Hoofdstuk 2 introduceerden we de codes $\mathcal{C}_k(n,q)$ en $\mathcal{C}_k(n,q)^\perp$. We bekeken ook enkele voorbeelden van codewoorden en definieerden belangrijke meetkundige structuren zoals k-blokkerende en even verzamelingen. In het volgende hoofdstuk leerden we dat het minimum gewicht van $\mathcal{C}_k(n,q)$ gelijk is aan θ_k. De minimum gewicht codewoorden zijn de scalaire veelvouden van incidentievectoren van k-ruimten. Daarna gingen we over naar het minimum gewicht van $\mathcal{C}_k(n,q)^\perp$. In het algemeen is het niet geweten wat dit is, maar we weten wel dat $d(\mathcal{C}_k(n,q)^\perp) = d(\mathcal{C}_1(n-k+1,q)^\perp)$. Voor q priem is bewezen dat dit minimum gewicht $2q^{n-k}$ is. De bijhorende codewoorden zijn het scalair veelvoud van het verschil van twee $(n-k)$-ruimten die snijden in een $(n-k-1)$-ruimte. Als q even is, vonden we dat het minimum gewicht gelijk is aan $q^{n-k-1}(q+2)$. Het bleek dat hypercilinders die een $(n-k+1)$-ruimte opspannen, de corresponderende codewoorden zijn voor $q=4$ en 8. Deze resultaten zouden kunnen doen vermoeden dat het minimum gewicht van $\mathcal{C}_k(n,q)^\perp$ gelijk is aan $q^{n-k-1}(q+p)$. Echter bij het vergelijken van verschillende ondergrenzen besloten we dat meestal de volgende ondergrens de beste is:

$$2\left(\theta_{n-k}\left(1-\frac{1}{p}\right)+\frac{1}{p}\right).$$

In Hoofdstuk 4 gingen we dieper in op de classificatie resultaten van de codewoorden met een klein gewicht van $\mathcal{C}_k(n,q)$. In detail hebben we het resultaat besproken over het lege interval

$$\left]\theta_k, 2\left(\theta_{n-k}\left(1-\frac{1}{p}\right)+\frac{1}{p}\right)\right[$$

in de verdeling van de gewichten als $p>5$. Hierbij gebruikten we een verband met k-blokkerende verzamelingen. We vermelden daarnaast dat voor q voldoende groot recent alle codewoorden met gewicht hoogstens ruwweg $3q^k$ en voor q niet priem tot ruwweg $\sqrt{q}q^k$, gekend zijn. Als $k=n-1$, heeft men zelfs voor q voldoende groot tot gewicht ruwweg $4q^{n-1}$ de codewoorden kunnen beschrijven. Wij hebben een kort bewijs besproken dat de classificatie van de codewoorden tot gewicht $2q^{n-1}$ van $\mathcal{C}_{n-1}(n,q)$ aantoont.

In Hoofdstuk 5 bewijzen we nieuwe resultaten over de karakterisering van de codewoorden met een klein gewicht van $\mathcal{C}_k(n,8)^\perp$, met $k\in\{1,\ldots,n-2\}$. Merk op dat het geweten is dat even verzamelingen overeenkomen met codewoorden van $\mathcal{C}_1(n,q)^\perp$ als q even is. Voor onze resultaten steunen we ook op de karakterisering van de minimum gewicht codewoorden. Zo kunnen we via verschillende stappen het bestaan van codewoorden met een beetje hoger gewicht uitsluiten. Eerst gebruikten we dat elk codewoord van $\mathcal{C}_k(n,q)^\perp$, met q even, een even gewicht heeft. Vervolgens bewezen we dat er geen even verzamelingen bestaan met grootte $q(q+2)+2$ in $\mathrm{PG}(3,q)$, met $q\in\{4,8\}$. We konden dit resultaat voor $q=8$ uitbreiden tot het niet-bestaan van een codewoord met gewicht $q(q+2)+2$ in de code $\mathcal{C}_{n-2}(n,q)^\perp$. Op zijn beurt konden we hiermee het bestaan van een codewoord met gewicht $q^{n-k-1}(q+2)+2$ uitsluiten voor $k\in\{1,\ldots,n-2\}$ en $q=8$ in de code $\mathcal{C}_k(n,q)^\perp$. Zo bekomen we dat er geen codewoorden zijn in $\mathcal{C}_k(n,8)^\perp$, als $k\in\{1,\ldots,n-2\}$, met gewicht in het open interval

$$]q^{n-k-1}(q+2), q^{n-k-1}(q+2)+4[.$$

Ten slotte bespreken we in het laatste hoofdstuk drie gerelateerde codes. We beginnen met de codes $\mathcal{C}_{j,k}(n,q)$ en zijn duale. Het minimum gewicht van $\mathcal{C}_{j,k}(n,q)$ is $\begin{bmatrix} k+1 \\ j+1 \end{bmatrix}_q$ en de minimum gewicht codewoorden zijn scalaire veelvouden van de karakteristieke vectoren van een k-ruimte. Als q voldoende groot is, zijn de codewoorden met gewicht hoogstens $\left(3-\frac{7}{q}\right)\begin{bmatrix} k+1 \\ j+1 \end{bmatrix}_q$ een lineaire combinatie van de karakteristieke vectoren van hoogstens twee k-ruimten. Opnieuw voor q niet priem en voldoende groot zijn er verdere karakteriseringsresultaten tot ruwweg gewicht $\sqrt{q}q^{k-j}$. Voor de duale code $\mathcal{C}_{j,k}(n,q)^\perp$ is het minimum gewicht gelijk aan dit van de code $\mathcal{C}_{0,1}(n-k+1,q)^\perp$. Het minimum gewicht is dus in het algemeen enkel geweten voor q priem of even.

Daarna hebben we in meer detail de codewoorden van $\mathcal{M}_{1,1}(3,q)$ bestudeerd tot en met gewicht q^3+2q^2+q+1 voor $q \geq 19$. Zo'n codewoord is het scalaire veelvoud van de karakteristieke vector van een rechte. Tenzij als q even is, want dan kan het codewoord ook een scalair veelvoud zijn van de karakteristieke vector van de verzameling absolute rechten van een symplectische polariteit. In dit geval is het minimum gewicht q^3+q^2+q+1 in plaats van q^3+2q^2+q+1. Het laatste voorbeeld was de code van klassieke polaire ruimten. Ter illustratie gaven we twee voorbeelden van codewoorden van de code $\mathcal{C}_2(Q^+(5,q))^\perp$.

We besluiten dat de codes komende van incidentiematrices een boeiend en hedendaags onderwerp is. De verbanden met de meetkundige structuren zorgen voor verschillende mooie resultaten. Ook zijn er nog vele richtingen mogelijk voor verder onderzoek. Bijvoorbeeld uitbreidingen van de gevonden resultaten in Hoofdstuk 5 voor grotere gewichten of andere even q. Men kan ook proberen om deze resultaten uit te breiden naar de code $\mathcal{C}_{j,k}(n,q)^\perp$. Daarnaast blijft het een interessante vraag wat in het algemeen het minimum gewicht is van de code $\mathcal{C}_k(n,q)^\perp$. Het feit dat dit doorheen de jaren nog niet gevonden is, doet vermoeden dat het geen eenvoudige formule zal zijn. Ook zijn er veel mogelijke andere relevante codes om te bestuderen, bijvoorbeeld $\mathcal{M}_{1,1}(3,q)^\perp$. Kortom, er zijn vele leuke onderzoeksrichtingen mogelijk.

A English summary

This thesis mainly concentrates on the codewords with small weight of the code $\mathcal{C}_k(n,q)$ and its dual $\mathcal{C}_k(n,q)^\perp$. The code $\mathcal{C}_k(n,q)$ is generated by the characteristic vectors of each k-space τ in $\mathrm{PG}(n,q)$. This is a vector indexed over all the points of $\mathrm{PG}(n,q)$. The value of a point is 1 if the point lies in the k-space τ and 0 otherwise. The resulting code is the $\mathbb{F}_p$-span of these vectors. Our goal is to acquire a better knowledge of the small weight codewords of $\mathcal{C}_k(n,q)$ and $\mathcal{C}_k(n,q)^\perp$.

The first thing that we studied is the minimum weight of $\mathcal{C}_k(n,q)$. It turns out that this is θ_k and that the minimum weight codewords are scalar multiples of the characteristic vectors of a k-space. We also looked at the codewords with a slightly higher weight. In particular, we discussed in detail the empty interval

$$\left]\theta_k, 2\left(\theta_{n-k}\left(1-\frac{1}{p}\right)+\frac{1}{p}\right)\right[$$

in the weight distribution of $\mathcal{C}_k(n,q)$ using the link with k-blocking sets. For $k=n-1$, we examined a short proof of the classification till the weight $2q^{n-1}$. We also mention that for q large enough and $k=n-1$ the codewords are studied in the literature till roughly weight $4q^{n-1}$ or $\sqrt{q}q^{n-1}$ for q not prime. For general k and q large enough the codewords are described till roughly the weight $3q^k$ and for q not prime till roughly weight $\sqrt{q}q^k$.

We also took a closer look at the minimum weight of $\mathcal{C}_k(n,q)^\perp$. It is in general not known what this weight is. We discussed three different lower bounds for this weight and concluded that in most cases the following bound gives the best results:

$$2\left(\theta_{n-k}\left(1-\frac{1}{p}\right)+\frac{1}{p}\right).$$

The minimum weight is known for q prime or even. In the first case it is equal to $2q^{n-k}$ and the minimum weight codewords are scalar multiples of two $(n-k)$-spaces that intersect in an $(n-k-1)$-space. When $q=4$ or 8, the minimum weight codewords are scalar multiples of a hypercilinder that spans an $(n-k+1)$-space. For other even q it is only known that the minimum weight is $q^{n-k-1}(q+2)$.

We did some new research on codewords of $\mathcal{C}_k(n,q)^\perp$ with weight slightly higher than the minimum weight for $q=8$. First we showed that there does not exist an even set with size $q(q+2)+2$ in $\mathrm{PG}(3,8)$. Since even sets correspond to codewords of $\mathcal{C}_1(n,q)^\perp$ for q even, this is equivalent to the non-existence of codewords with weight $q(q+2)+2$ of $\mathcal{C}_1(3,8)^\perp$. We were also able to enclose the support of the codewords with weight $q(q+2)+2$ of $\mathcal{C}_{n-2}(n,8)^\perp$ in a space of dimension at most 4. Using these things and exploiting the form of the minimum weight codewords we eliminated the codewords with weight $q(q+2)+2$ of the code $\mathcal{C}_{n-2}(n,8)^\perp$. Afterwards, we could extend this result to rule out the existence of codewords with weight $q^{n-k-1}(q+2)+2$ in the code $\mathcal{C}_k(n,8)^\perp$, $k\in\{1,\ldots,n-2\}$. We also verified that the codewords of $\mathcal{C}_k(n,q)^\perp$ have even weight when q is even. So we find the following empty interval

$$]q^{n-k-1}(q+2), q^{n-k-1}(q+2)+4[$$

in the weight distribution of the code $\mathcal{C}_k(n,8)^\perp$, for $k\in\{1,\ldots,n-2\}$.

In the last chapter we introduced three related codes. The codes $\mathcal{C}_{j,k}(n,q)$ and $\mathcal{M}_{j,k}(n,q)$ are both generated by the characteristic vectors of k-spaces. However the meaning of a characteristic vector is different. Both are indexed over the j-spaces in $\mathrm{PG}(n,q)$. In the first case we place a 1 when the j-space is contained in the k-space and otherwise 0. For the second code we only require a non-empty intersection with the j-space and the k-space to place a 1. Note that $\mathcal{C}_{0,k}(n,q) = \mathcal{M}_{0,k}(n,q) = \mathcal{C}_k(n,q)$. For $\mathcal{C}_{j,k}(n,q)$ we require $0 \leq j < k \leq n-1$, while for $\mathcal{M}_{j,k}(n,q)$ we have $0 \leq j,k \leq n-1$. The codewords of the code $\mathcal{C}_{j,k}(n,q)$ for q large enough are studied till weight $\left(3-\frac{7}{q}\right)\begin{bmatrix}k+1\\j+1\end{bmatrix}_q$. The minimum weight codewords are scalar multiples of the characteristic vector of a k-space. Thus the minimum weight itself is $\begin{bmatrix}k+1\\j+1\end{bmatrix}_q$. For q not prime and large enough the codewords are examined till roughly weight $\sqrt{q}q^{k-j}$. Again the results for the dual code are harder to find. It turns out that $d(\mathcal{C}_{j,k}(n,q)^\perp) = d(\mathcal{C}_{0,1}(n-k+1,q))^\perp$. This means that we know for q prime that $d(\mathcal{C}_{j,k}(n,q)^\perp) = 2q^{n-k}$ and for q even the minimum weight is $q^{n-k-1}(q+2)$.

We also looked at the characterisation of the minimum weight codewords of the code $\mathcal{M}_{1,1}(3,q)$. An interesting result is that the characteristic vector of the absolute lines of a symplectic polar space $W(3,q)$ is a codeword of $\mathcal{M}_{1,1}(3,q)$ if and only if q is even. We call the code generated from these codewords and $\mathcal{M}_{1,1}(3,q)$ the code $\mathcal{M}(3,q)$. The characterisation of the codewords with weight at most q^3+2q^2+q+1 for $q \geq 19$ of the code $\mathcal{M}(3,q)$ is known. These are the scalar multiples of the characteristic vector of a line or the characteristic vector of the absolute lines of a symplectic polar space $W(3,q)$. Since $\mathcal{M}_{1,1}(3,q) \subseteq \mathcal{M}(3,q)$, the code $\mathcal{M}_{1,1}(3,q)$ is characterised as well for $q \geq 19$.

Finally, we mentioned that we can restrict the incidence matrix of $\mathcal{C}_k(n,q)$ to all k-spaces of a certain structure, for instance a classical polar space. In particular we examined two small weight codewords of $\mathcal{C}_2(Q^+(5,q))^\perp$. These examples illustrate that there are many related codes to $\mathcal{C}_k(n,q)$ and $\mathcal{C}_k(n,q)^\perp$ that can be studied. With this in mind, we conclude our overview of the main topics and results that are discussed in this thesis.

Bibliografie

[1] S. Adriaensen. “A note on small weight codewords of projective geometric codes and on the smallest sets of even type”. In: *SIAM J. Discrete Math.* 37.3 (2023), p. 2072–2087.

[2] S. Adriaensen en L. Denaux. “Small weight codewords of projective geometric codes”. In: *J. Combin. Theory Ser. A* 180 (2021), Paper No. 105395, 34.

[3] S. Adriaensen en L. Denaux. “Small weight codewords of projective geometric codes II”. In: *Des. Codes and Cryptogr.* (2024), p. 1–22.

[4] S. Adriaensen, L. Denaux, L. Storme en Zs. Weiner. “Small weight code words arising from the incidence of points and hyperplanes in $\mathrm{PG}(n, q)$”. In: *Des. Codes Cryptogr.* 88.4 (2020), p. 771–788.

[5] S. Adriaensen, J. Mannaert, P. Santonastaso en F. Zullo. “Cones from maximum h-scattered linear sets and a stability result for cylinders from hyperovals”. In: *Discrete Math.* 346.12 (2023), Paper No. 113602, 18.

[6] S. Adriaensen, R. Simoens en L. Storme. *The minimum weight of the code of intersecting lines in* $\mathrm{PG}(3, q)$. 2024. arXiv: 2403.07451 [math.CO].

[7] E. F. Assmus Jr. en J. D. Key. *Designs and their codes*. Deel 103. Cambridge Tracts in Mathematics. Cambridge University Press, Cambridge, 1992, p. x+352.

[8] B. Bagchi en S. P. Inamdar. “Projective geometric codes”. In: *J. Combin. Theory Ser. A* 99.1 (2002), p. 128–142.

[9] D. Bartoli en L. Denaux. “Minimal codewords arising from the incidence of points and hyperplanes in projective spaces”. In: *Adv. Math. Commun.* 17.1 (2023), p. 56–77.

[10] R. C. Bose en R. C. Burton. “A characterization of flat spaces in a finite geometry and the uniqueness of the Hamming and the MacDonald codes”. In: *J. Combinatorial Theory* 1 (1966), p. 96–104.

[11] A. E. Brouwer, A. M. Cohen en A. Neumaier. *Distance-regular graphs*. Deel 18. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]. Springer-Verlag, Berlin, 1989, p. xviii+495.

[12] A. Bruen. “Blocking sets in finite projective planes”. In: *SIAM J. Appl. Math.* 21 (1971), p. 380–392.

[13] N. J. Calkin, J. D. Key en M. J. de Resmini. “Minimum weight and dimension formulas for some geometric codes”. In: *Des. Codes Cryptogr.* 17.1-3 (1999), p. 105–120.

[14] M. De Boeck. “Small weight codewords in the dual code of points and hyperplanes in $\mathrm{PG}(n, q)$, q even”. In: *Des. Codes Cryptogr.* 63.2 (2012), p. 171–182.

[15] M. De Boeck en P. Vandendriessche. “On the dual code of points and generators on the Hermitian variety $\mathcal{H}(2n + 1, q^2)$”. In: *Adv. Math. Commun.* 8.3 (2014), p. 281–296.

[16] M. De Boeck en G. Van de Voorde. “Embedded antipodal planes and the minimum weight of the dual code of points and lines in projective planes of order p^2”. In: *Des. Codes Cryptogr.* 91.3 (2023), p. 895–920.

[17] L. Denaux. "Characterising and constructing codes using finite geometries". Proefschrift. Ghent University, 2023.

[18] N. Hamada. "The rank of the incidence matrix of points and d-flats in finite geometries". In: *J. Sci. Hiroshima Univ. Ser. A-I Math.* 32 (1968), p. 381–396.

[19] N. V. Harrach, K. Metsch, T. Szőnyi en Zs. Weiner. "Small point sets of $\mathrm{PG}(n, p^{3h})$ intersecting each line in $1 \bmod p^h$ points". In: *J. Geom.* 98.1-2 (2010), p. 59–78.

[20] J. W. P. Hirschfeld. *Projective geometries over finite fields.* Tweede editie. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1998, p. xiv+555.

[21] J. W. P. Hirschfeld en X. Hubaut. "Sets of even type in $\mathrm{PG}(3, 4)$, alias the binary (85, 24) projective geometry code". In: *J. Combin. Theory Ser. A* 29.1 (1980), p. 101–112.

[22] M. Lavrauw, L. Storme, P. Sziklai en G. Van de Voorde. "An empty interval in the spectrum of small weight codewords in the code from points and k-spaces of $\mathrm{PG}(n, q)$". In: *J. Combin. Theory Ser. A* 116.4 (2009), p. 996–1001.

[23] M. Lavrauw, L. Storme en G. Van de Voorde. "A proof of the linearity conjecture for k-blocking sets in $\mathrm{PG}(n, p^3)$, p prime". In: *J. Combin. Theory Ser. A* 118.3 (2011), p. 808–818.

[24] M. Lavrauw, L. Storme en G. Van de Voorde. "Linear codes from projective spaces". In: *Error-correcting codes, finite geometries and cryptography.* Deel 523. Contemp. Math. Amer. Math. Soc., Providence, RI, 2010, p. 185–202.

[25] M. Lavrauw, L. Storme en G. Van de Voorde. "On the code generated by the incidence matrix of points and hyperplanes in $\mathrm{PG}(n, q)$ and its dual". In: *Des. Codes Cryptogr.* 48.3 (2008), p. 231–245.

[26] M. Lavrauw, L. Storme en G. Van de Voorde. "On the code generated by the incidence matrix of points and k-spaces in $\mathrm{PG}(n, q)$ and its dual". In: *Finite Fields Appl.* 14.4 (2008), p. 1020–1038.

[27] F. J. MacWilliams en N. J. A. Sloane. *The theory of error-correcting codes. I.* Deel 16. North-Holland Mathematical Library. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977, i–xv en 1–369.

[28] F. J. MacWilliams en N. J. A. Sloane. *The theory of error-correcting codes. II.* Deel 16. North-Holland Mathematical Library. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977, i–ix en 370–762.

[29] R. J. McEliece. "Weight congruences for p-ary cyclic codes". In: *Discrete Math.* 3.1 (1972), p. 177–192.

[30] S. Packer. "On sets of odd type and caps in Galois geometries of order four." Proefschrift. University of Sussex, 1995.

[31] V. Pepe, L. Storme en G. Van de Voorde. "On codewords in the dual code of classical generalised quadrangles and classical polar spaces". In: *Discrete Math.* 310.22 (2010), p. 3132–3148.

[32] V. Pepe, L. Storme en G. Van de Voorde. "Small weight codewords in the LDPC codes arising from linear representations of geometries". In: *J. Combin. Des.* 17.1 (2009), p. 1–24.

[33] W. W. Peterson en E. J. Weldon Jr. *Error-correcting codes.* Tweede editie. The M.I.T. Press, Cambridge, Mass.-London, 1972, p. xi+560.

[34] O. Polverino en F. Zullo. "Codes arising from incidence matrices of points and hyperplanes in $\mathrm{PG}(n, q)$". In: *J. Combin. Theory Ser. A* 158 (2018), p. 1–11.

[35] B. Segre. "Sui k-archi nei piani finiti di caratteristica due". In: *Rev. Math. Pures Appl.* 2 (1957), p. 289–300.

[36] P. Sin. "The p-rank of the incidence matrix of intersecting linear subspaces". In: *Des. Codes Cryptogr.* 31.3 (2004), p. 213–220.

[37] D. R. Stinson. "Nonincident points and blocks in designs". In: *Discrete Math.* 313.4 (2013), p. 447–452.

[38] L. Storme. *Codeertheorie*. Universiteit Gent, 2022-2023.

[39] L. Storme. *Galoismeetkunde*. Universiteit Gent, 2022-2023.

[40] T. Szőnyi en Zs. Weiner. "Stability of $k \bmod p$ multisets and small weight codewords of the code generated by the lines of $\mathrm{PG}(2, q)$". In: *J. Combin. Theory Ser. A* 157 (2018), p. 321–333.

[41] T. Szőnyi en Zs. Weiner. "Small blocking sets in higher dimensions". In: *J. Combin. Theory Ser. A* 95.1 (2001), p. 88–101.

[42] M. Tallini Scafati. "Caratterizzazione grafica delle forme hermitiane di un $S_{r,q}$". In: *Rend. Mat. e Appl. (5)* 26 (1967), p. 273–303.

[43] P. Vanden Eede. "Higgledy-piggledy verzamelingen in eindige projectieve ruimten". Bachelorproef. Universiteit Gent, 2021-2022.