Antwoorden van het Tentamen Discrete Wiskunde 2
27 juni 2012, 14:00–17:00 uur

Maarten Solleveld

Opgave 1. (4 punten)
Zij $\mathcal{F} = (A_1, A_2, \ldots, A_n)$ een familie deelverzamelingen van $\{1, 2, \ldots, n\}$ met incidentiematrix $M \in M_n(\mathbb{Z})$.

a. Toon aan dat $\mathcal{F}$ minstens $|\det M|$ volledige matchings heeft.

b. Geef een voorbeeld waarin $|\det M| > 1$ en het aantal volledige matchings precies $-\det M$ is.

Oplossing
1.a. (2 punten)
Per definitie $M_{ij} \in \{0, 1\}$ en

$$\det M = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^{n} M_{i\sigma(i)}.$$

Dus er zijn minstens $|\det M|$ permutaties $\sigma \in S_n$ zodat $M_{i\sigma(i)} = 1$ voor alle i. Dat betekent $i \in A_{\sigma(i)}$ en $\sigma^{-1}(i) \in A_i$ voor alle i, dus elk zo'n σ levert een volledige matching van deze familie.
Alternatieve methode: Het aantal volledige matchings is de permanent van de incidentiematrix M. Uit

$$\text{per } M = \sum_{\sigma \in S_n} \prod_{i=1}^{n} M_{i\sigma(i)}$$

en $M_{ij} \geq 0$ volgt dat $\text{per}(M) \geq |\det(M)|$. *De voorwaarde $M_{ij} \geq 0$ werd meerdere keren vergeten maar is wel nodig, zie de matrix* $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$.
1.b. (2 punten)
Het eenvoudigste voorbeeld is $n = 3$, $A_1 = \{1, 2\}$, $A_2 = \{1, 3\}$ en $A_3 = \{2, 3\}$. Dan $M = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$, $\det M = -2$ en er zijn precies twee volledige matchings, namelijk $(1, 3, 2)$ en $(2, 1, 3)$.

Opgave 2. (5 punten)
Zij X een verzameling met v elementen en zij $\mathcal{B}$ een familie blokken $B \subset X$ met $|B| = k$ en $|\mathcal{B}| = v$. We nemen aan dat elke twee blokken een doorsnede van precies één punt hebben.

a. Bewijs dat $(X, \mathcal{B})$ een $1 - (v, k, k)$-design is.

b. Laat zien dat $(X, \mathcal{B})$ een projectief vlak van orde $k - 1$ is.

Oplossing
2.a. (3 punten)
Het enige dat aangetoond moet worden is: voor elke $x \in X$ geldt $r_x = k$. We kiezen een x en onderscheiden twee gevallen: x ligt in alle blokken, of niet.
Geval 1 : $x \in B$ voor alle $B \in \mathcal{B}$. Dan is de doorsnede van elke twee blokken precies $\{x\}$, dus $B \setminus \{x\}$ en $B' \setminus \{x\}$ zijn disjunct. Het aantal punten in alle blokken samen is dus

$$1 + \sum_{B \in \mathcal{B}} |B \setminus \{x\}| = 1 + v(k-1) \leq |X| = v.$$

Dit kan alleen als $k = 1$. Maar dan zijn alle blokken gelijk aan $\{x\}$, dus $1 = |\mathcal{B}| = v$ en $X = \{x\}$. In dit geval hebben we te maken met een $1-(1,1,1)$-design. Flauw maar mogelijk.
Geval 2 : Er is een blok B_0 dat x niet bevat. Een blok B dat x wel bevat snijdt B_0 in een uniek punt, zeg $s(B)$. Als ook $x \in B'$, dan $s(B') \neq s(B)$ omdat $B \cap B' = \{x\}$. Dus $B \mapsto s(B)$ is een injectieve afbeelding van de verzameling blokken die x bevatten naar B_0. Hieruit volgt $r_x \leq k$.

Aangezien dit voor willekeurige $x \in X$ gedaan kan worden geldt

$$vk = \sum_{B \in \mathcal{B}} |B| = \sum_{x \in X} r_x \leq |X|k = vk,$$

Omdat de uitersten gelijk zijn, moet wel $r_x = k$ voor alle $x \in X$.
Veel gemaakte fout: Neem aan dat $(X, \mathcal{B})$ een design is. Dit is niet gegeven en mag dus niet gebruikt worden!
2.b. (2 punten)
Elke lijn heeft duidelijk $(k-1)+1$ elementen, dus we moeten nog aantonen dat $v = (k-1)^2 + (k-1) + 1 = k^2 - k + 1$, en dat elke twee punten op een unieke lijn liggen. Beschouw triples (B, x, B') met $x = B \cap B'$ en $B, B' \in \mathcal{B}$. Door naar de blokken te kijken zien we dat er hiervan $\binom{v}{2}$ zijn. Anderszijds kunnen we voor elke $x \in X$ precies $\binom{r_x}{2} = \binom{k}{2}$ paren van blokken met deze eigenschap vinden, dus het aantal triples is ook $|X|\binom{k}{2}$. Hieruit volgt

$$v(v-1) = |X|k(k-1) = vk(k-1) \quad \text{en} \quad v = k(k-1) + 1 = k^2 - k + 1.$$

Uit de gegevens zien we dat elk paar in X in ten hoogstens één blok ligt. Het aantal paren in X is $\binom{v}{2}$ en het aantal paren dat in een blok ligt is $|\mathcal{B}|\binom{|B|}{2} = v\binom{k}{2}$. Volgens de bovenstaande berekening zijn deze twee aantallen gelijk, dus elke twee elementen van X liggen in een uniek blok.
Bij de opgave werd meerdere malen aangenomen dat het al een 2-design, en dan ben je snel klaar. Maar niet elk 1-design is een 2-design, dus dat moest eerst bewezen worden.

Opgave 3. (8 punten)
Een quasigroep $(G, \circ)$ heet *idempotent* als $x \circ x = x$ voor alle $x \in G$. Verder heet $(G, \circ)$ *commutatief* als $x \circ y = y \circ x$ voor alle $x, y \in G$.

a. Geef voor elke oneven $m \in \mathbb{N}$ een commutatieve idempotente quasigroep van orde m.

b. Zij D_{2n} de verzameling van commutatieve quasigroepen op $\{1, 2, \ldots, 2n\}$, zodat $x \circ x = 2n$ voor alle x.
Geef een bijectie tussen D_{2n} en de collectie van commutatieve idempotente quasigroepen met onderliggende verzameling $\{1, 2, \ldots, 2n-1\}$.

c. Zij $q \geq 5$ een oneven priemmacht. Vind Latijnse vierkanten L en S van grootte q, zodat S hoort bij een commutatieve idempotente quasigroep en L orthogonaal staat op L^T en op S.

Hint: pas de optelling in $\mathbb{F}_q$ op geschikte wijze aan.

Oplossing

3.a. (2 punten)

Neem als verzameling $\mathbb{Z}/m\mathbb{Z}$ en als operatie $x \circ y = (x+y)/2$. Dit mag omdat 2 inverteerbaar is in $\mathbb{Z}/m\mathbb{Z}$, en het is duidelijk dat deze operatie commutatief en idempotent is. De vergelijking $x \circ y = z$ (met y vast) een unieke oplossing, namelijk $x = 2z - y$. Voor x vast gaat het net zo, dus het is echt een quasigroep.

3.b. (2 punten)

Dit is inzichtelijker als we het met Latijnse vierkanten doen. Bij zo een commutatieve idempotente quasigroep hoort een symmetrische Latijns vierkant van de vorm

$$C = \begin{pmatrix} 1 & & \cdots & \\ & 2 & c_{i,j} & \\ \vdots & & \ddots & \\ & & & 2n-1 \end{pmatrix}$$

en elk element van D_{2n} correspondeert met een symmetrisch Latijns vierkant

$$D = \begin{pmatrix} 2n & & \cdots & & d_{1,2n} \\ & 2n & d_{i,j} & & d_{2,2n} \\ \vdots & & \ddots & & \\ & & & 2n & d_{2n-1,2n} \\ d_{1,2n} & d_{2,2n} & & d_{2n-1,2n} & 2n \end{pmatrix}.$$

We sturen C naar de matrix D met $d_{i,i} = 2n$, $d_{j,2n} = j$ en $d_{i,j} = c_{i,j}$ in alle andere gevallen. De afbeelding in de omgekeerde richting is ietsje lastiger. Omdat D een Latijns vierkant is, bestaat er een unieke $\sigma \in S_{2n-1}$ zodat $\sigma(d_{i,2n}) = i$ voor alle $i < 2n$. Deze permutatie van de symbolen verandert D niet wezenlijk, maar brengt haar wel in de vorm

$$D^\sigma = \begin{pmatrix} 2n & & \cdots & & 1 \\ & 2n & d^\sigma_{i,j} & & 2 \\ \vdots & & \ddots & & \\ & & & 2n & 2n-1 \\ 1 & 2 & & 2n-1 & 2n \end{pmatrix}.$$

Nu sturen we D^σ naar de matrix C met $c_{i,i} = i$ en $c_{i,j} = d^\sigma_{i,j}$ voor alle overige coëfficiënten. Het is eenvoudig in te zien dat deze twee afbeeldingen elkaars inverse zijn en dat ze de eigenschappen van een Latijns vierkant bewaren.

3.c. (4 punten)

Voor S nemen we het Latijnse vierkant bij de quasigroep met verzameling $\mathbb{F}_q$ en bewerking $x \circ_S y = (x+y)/2$. Net als in deel a gaat dit goed doordat 2 inverteerbaar is in $\mathbb{F}_q$.

Omdat $q > 3$ is er een $\lambda \in \mathbb{F}_q \setminus \{1, 0, -1\}$. Bij L nemen we de quasigroep met verzameling $\mathbb{F}_q$ en operatie $x \circ_L y = x + \lambda y$. Dit is een quasigroep doordat λ inverteerbaar is. Merk op dat L, via het procedé van opgave 5, de lijnen in $\mathbb{A}^2(\mathbb{F}_q)$ met richtingscoëfficiënt λ beschrijft.

De operatie van de quasigroep die hoort bij L^T is dan $x \circ_L^T y = \lambda x + y$. We moeten aantonen dat deze drie quasigroepen / Latijnse vierkanten paarsgewijs orthogonaal zijn. Dit kan je al zien doordat ze lijnen in $\mathbb{A}^2(\mathbb{F}_q)$ van verschillende richtingen beschrijven, maar laten we het ook uitwerken. Voor $(a, b) \in \mathbb{F}_q$ zoeken we oplossingen van $x \circ_S y = a$ en $x \circ_L y = b$. Met een beetje rekenen zien we dat er precies eentje is, namelijk

$$y = \frac{b - 2a}{\lambda - 1}, \; x = \frac{2a\lambda - b}{\lambda - 1}.$$

Dus L en S zijn orthogonaal. Ook het paar vergelijkingen $x \circ_L^T y = a$ en $x \circ_L y = b$ heeft een unieke oplossing, en wel

$$y = \frac{a - \lambda b}{1 - \lambda^2}, \; x = \frac{b - \lambda a}{1 - \lambda^2}.$$

Hier gebruiken we dat $\lambda^2 \neq 1$ (wat kon doordat $q > 3$).

Opgave 4. (10 punten)

Zij $(X, \mathcal{B})$ een Steiner triple systeem van grootte v. Zij $S \subset X$ een deelverzameling met de eigenschap dat $S \cap B \neq \emptyset$ voor elk triple $B \in \mathcal{B}$.

a. Vind, in het geval dat $(X, \mathcal{B}) = \mathbb{A}^2(\mathbb{F}_3)$, de minimale grootte van zo'n S.

b. Toon aan dat $|S| \geq (v - 1)/2$.

c. Neem aan dat $|S| = (v - 1)/2$. Bewijs dat $\big(S, \{B \in \mathcal{B} \mid B \subset S\}\big)$ een Steiner triple systeem is.

Oplossing.

4.a. (3 punten)

$X = (\mathbb{Z}/3\mathbb{Z})^2$ en $\mathcal{B}$ is de verzameling van affiene lijnen $ax + by = c$ in X. Een geschikte deelverzameling S van grootte 5 is $\{(0,0), (1,0), (-1,0), (0,1), (0,-1)\}$. We willen inzien dat het niet met minder dan 5 elementen lukt. We weten dat er 12 lijnen zijn en dat elk punt op 4 lijnen ligt. Elk tweetal punten $x_1, x_2 \subset S$ ligt niet op 8 lijnen maar op 7, want er is een lijn die ze allebei bevat.

Stel eerst dat x_3 op deze ene lijn ligt. Dan bestaat $X \setminus \{x_1, x_2, x_3\}$ uit twee parallelle lijnen. Dus hebben we minstens twee punten nodig om $\{x_1, x_2, x_3\}$ uit te breiden tot een verzameling die alle lijnen van X treft.

Neem nu aan dat x_3 niet op de lijn door x_1, x_2 ligt. Dan zijn er precies drie lijnen die een tweetal uit $\{x_1, x_2, x_3\}$ bevatten, dus x_1, x_2, x_3 liggen samen op $3 \cdot 4 - 3 = 9$

lijnen. Een willekeurig vierde punt x_4 ligt op een lijn met x_1, een lijn met x_2 en een lijn met x_3. Deze laatste drie lijnen kunnen niet allemaal hetzelfde zijn (want dan zouden er vier punten op liggen), dus x_4 ligt op minstens twee lijnen die we al hadden door $\{x_1, x_2, x_3\}$. Omdat x_4 zelf op 4 lijnen ligt, zijn daarvan hoogstens twee nieuw. In totaal liggen x_1, x_2, x_3, x_4 dus op hoogstens 11 lijnen. Met vier punten kunnen we daarom niet alle 12 lijnen van $\mathbb{A}^2(\mathbb{F}_3)$ treffen.

Alternatieve methode: bekijk drie punten probeer ze aan te vullen tot zo een S. De groep $\mathbb{F}_3^2 \rtimes GL_2(\mathbb{F}_3)$ van affiene transformaties werkt op $\mathbb{A}^2(\mathbb{F}_3)$ door symmetrieën van dit design. Modulo deze werking zijn er slechts twee wezenlijk verschillende configuraties van drietallen in $\mathbb{A}^2(\mathbb{F}_q)$, namelijk allemaal op een lijn of niet. Het volstaat dus om de drietallen $\{(0,0),(1,0),(-1,0)\}$ en $\{(0,0),(1,0),(0,1)\}$ te bekijken. Nu zie je door het uit proberen gemakkelijk dat S minstens 5 punten moet hebben.

Veel gemaakte fout: laat wel zien dat $|S| \geq 4$, maar controleer niet of het echt kan met 4 elementen.

4.b. (3 punten)

Als $S = X$ dan zijn we direct klaar, dus we mogen aannemen dat er een $x \in X \setminus S$ is. Elk ander element $y \in X$ ligt samen met x in een uniek triple $B_y \in \mathcal{B}$. Voor een derde element $y' \in X$ geldt $B'_y = B_y$ (als $y' \in B_y$) of $B'_y \cap B_y = \{x\}$ (als $y' \notin B_y$). Dus er zijn $(v-1)/2$ triples B_y die x bevatten, en de verzamelingen $B_y \setminus \{x\}$ vormen een partitie van $X \setminus \{x\}$. Uit elk van deze triples B_y bevat S een punt s_y, en niet x. Dus de s_y zijn allemaal verschillend en $|S| \geq (v-1)/2$.

4.c. (4 punten)

Zij $\{s_1, s_2\}$ een willekeurig paar in S. Dan is er een uniek triple $B \in \mathcal{B}$ dat s_1 en s_2 bevat, zeg $B = \{s_1, s_2, x\}$. We moeten bewijzen dat $B \subset S$, ofwel dat $x \in S$. Stel dat in tegendeel $x \in X \setminus S$. In het bewijs van 4.b hebben we gezien dat x bevat is in $(v-1)/2$ triples uit $\mathcal{B}$ en dat S uit elk van deze triples minstens één punt bevat. Maar S bevat twee elementen van het triple B, dus in totaal heeft S minstens $(v-1)/2+1$ elementen. Tegenspraak met de aanname $|S| = (v-1)/2$.

Opgave 5. (12 punten)

Zij X een eindige verzameling met een familie $\mathcal{L}$ van lijnen $L \subset X$, en zij $k, r, \alpha \in \mathbb{N}$. Dan heet $(X, \mathcal{L})$ een *partiële meetkunde* met parameters (k, r, α) als:

- elke twee punten van X liggen op hoogstens één lijn;
- elke lijn heeft k punten;
- elke punt ligt op r lijnen;
- als $P \in X \setminus L$, dan zijn er precies α lijnen door P die L snijden.

Dit begrip generaliseert de affiene en projectieve meetkundes.

a. Bepaal (k, r, α) voor $\mathbb{A}^n(\mathbb{F}_q)$.

b. Gegeven zijn d paarsgewijs orthogonale Latijnse vierkanten $R^{(s)}$ van grootte n.

In $X = \{1, 2, \ldots, n\}^2$ definiëren we de lijnen

$$\begin{aligned} H_j &= \{(i, j) \mid 1 \le i \le n\}, \\ V_i &= \{(i, j) \mid 1 \le j \le n\}, \\ L_k^{(s)} &= \{(i, j) \mid R_{i,j}^{(s)} = k\}. \end{aligned}$$

Zij $\mathcal{L}$ de collectie van al deze $n(d+2)$ lijnen. In het college is (in andere terminologie) bewezen dat $(X, \mathcal{L})$ een partiële meetkunde is. Bepaal de parameters (k, r, α).

c. Neem nu n even, $d = n/2 - 2$ en fixeer $y \neq z \in X$. We noemen twee punten van X *collineair* als ze ongelijk zijn en in een lijn uit $\mathcal{L}$ liggen.

   Laat zien dat voor precies $n^2/2$ elementen $x \in X$ geldt: x is collineair met y of z, maar niet met allebei.

d. Zij A de $n^2 \times n^2$-matrix met kolommen en rijen geïndiceerd door X, zodat

$$A_{x,y} = \begin{cases} 1 & \text{als } x \text{ en } y \text{ collineair zijn} \\ -1 & \text{anders.} \end{cases}$$

   Laat zien dat A een Hadamard matrix is.

Oplossing.
5.a. (3 punten)
Een affiene lijn over $\mathbb{F}_q$ heeft $k = q$ elementen.
Laten we de lijnen door $0 \in \mathbb{F}_q^n$ tellen. Elk zo'n lijn wordt vastgelegd door een ander punt, en daarvan zijn er $q^n - 1$. Op deze manier krijgen we elke lijn door 0 $q - 1$ keer, dus het aantal lijnen door 0 is $r = \frac{q^n-1}{q-1}$.
Zij L een affiene lijn en $P \in \mathbb{F}_q^n \setminus L$. Voor elk punt $Q \in L$ is er een unieke lijn L_Q door P en Q. Als ook $Q' \in L$ en $L'_Q = L_Q$, dan $|L_Q \cap L| \ge 2$ dus $L_Q = L$ en $P \notin L$. Dat kan niet, dus $L'_Q \neq L_Q$. Het aantal lijnen door P dat L snijdt is dus gelijk aan het aantal punten van L, namelijk q.
Sommige studenten namen hier (impliciet) aan dat $n = 2$. Dat maakt voor k en α niet uit, maar voor r maakt het de vraag duidelijk makkelijker.
5.b. (2 punten)
Het is duidelijk dat $|H_j| = |V_i| = n$, dus $k = n$. Ook $|L_k^{(s)}| = n$, omdat $R^{(s)}$ een Latijns vierkant is.
Een punt (i, j) ligt op één lijn uit ieder van de klassen H_*, V_* en $L_*^{(s)}$, dus ligt in totaal op $r = d + 2$ lijnen.
Zij nu L een willekeurige lijn en $P \in X \setminus L$. Omdat we mogen aannemen dat $(X, \mathcal{L})$ een partiële meetkunde is, kunnen we α bepalen door te kijken naar het speciale geval $L = H_1, P = (2, 2)$. Dan ligt P op H_2, V_2 en op d lijnen $L_k^{(s)}$. Van deze $d + 2$ lijnen is alleen H_2 parallel met L, dus er zijn $\alpha = d + 1$ lijnen door P die L snijden.
5.c. (5 punten)
We onderscheiden of y en z wel of niet collineair zijn.
Geval 1 : y en z zijn niet collineair.
Uit deel b weten we dat $r = n/2$ en $\alpha = n/2 - 1$. Het punt y ligt op $n/2$ lijnen, die

elk y en $n-1$ andere punten bevatten. Dus y is collineair met $(n-1)n/2$ punten. We gaan tellen hoeveel punten hiervan ook collineair met z zijn. Voor elke lijn L door y geldt $z \notin L$, dus er zijn $\alpha = n/2 - 1$ lijnen door z die L snijden. Dit levert α punten op L die collineair met y en z zijn. Voor een lijn $L' \neq L$, ook door y, krijgen we weer α zulke punten. Deze twee verzamelingen van α punten zijn disjunct omdat $L' \cap L = \{y\}$. In totaal zijn er dus $\alpha n/2 = (n/2-1)n/2$ punten collineair met y en met z. Het aantal punten dat collineair met y maar niet met z is wordt daarmee

$$(n-1)n/2 - (n/2-1)n/2 = (n/2)n/2 = n^2/4.$$

Net zo zijn er $n^2/4$ punten collineair met z maar niet met y. Samen levert dit $n^2/2$ punten op die collineair met precies één van y en z zijn.
Geval 2 : y en z zijn collineair.
Dan liggen ze op een unieke lijn, zeg L_0. Op L_0 ligt precies één punt dat wel y maar niet met z collineair is, namelijk z. Er zijn $n/2-1$ andere lijnen L door y. Van zo'n lijn zijn de $n-1$ punten $L \setminus \{y\}$ collineair met y. Er zijn α lijnen door z die L snijden. Een daarvan is L_0, met snijpunt $L \cap L_0 = \{y\}$. De andere $\alpha - 1 = n/2 - 2$ lijnen door z leveren $n/2-2$ punten van $L \setminus \{y\}$ die collineair met y en met z zijn. In totaal geeft dit

$$1 + (n-1)(n/2-1) - (n/2-2)(n/2-1) = 1 + (n/2+1)(n/2-1) = n^2/4$$

punten die wel met y maar niet met z collineair zijn. Net zo zijn precies $n^2/4$ punten collineair met z maar niet met y.

5.d. (2 punten)

We moeten aantonen dat $AA^T = n^2 I$. Zij A_y een kolom van A. Omdat $A_{x,y} \in \{1,-1\}$ geldt

$$\langle A_y, A_y \rangle = \sum_{x \in X} A_{x,y}^2 = n^2.$$

Neem nu y en z verschillend. Vanwege deel c geldt $A_{x,y} = -A_{x,z}$ voor precies $n^2/2$ elementen $x \in X$. Dus $A_{x,y} = A_{x,z}$ voor de overige $n^2/2$ elementen $x \in X$. Hieruit volgt

$$\langle A_y, A_z \rangle = \sum_{x \in X} A_{x,y} A_{x,z} = n^2/2 \cdot -1 + n^2/2 = 0.$$

Deze twee vergelijkingen betekenen samen dat $AA^T = n^2 I$, dus A is een Hadamard matrix.