Examen G0Q98 Discrete Wiskunde. 8 juni 2018

Vraag 1 wordt mondeling besproken vanaf 10u00. De andere vragen zijn zuiver schriftelijk. Het ganse examen is open boek. Gelieve bij het indienen je antwoordbladen te nummeren en op elk blad je naam te schrijven.

Veel succes!

---

1. (a) Beschouw een eindig veld $\mathbb{F}_q$ en zij $\alpha \in \overline{\mathbb{F}}_q^\times$ een element met multiplicatieve orde n. Zij m de multiplicatieve orde van q modulo n en zij $g(x) \in \mathbb{F}_q[x]$ de minimale veelterm van α over $\mathbb{F}_q$. Dan wordt op en tussen de lijnen van pagina's 55-57 beweerd dat
   (i) $\deg g(x) = m$,
   (ii) $g(x) \mid x^n - 1$,
   (iii) de cyclische $(n, n-m)$-code $C \subset \mathbb{F}_q[x]/(x^n-1) \cong \mathbb{F}_q^n$ met generatorveelterm $g(x)$ bevat zit "in de kern van $\begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \end{pmatrix}$".

   Leg deze uitspraken in meer detail uit.

   (b) Zij K een veld en zij E/K een elliptische kromme met basispunt $\mathcal{O} \in E(K)$, in de zin van Definitie 6.20 uit de cursus. Beschrijf een meetkundige constructie aan de hand van raaklijnen en koordes om de inverse van een gegeven punt $\mathcal{P} \in E$ te bepalen.

2. Pollards $(p-1)$-methode voor het factoriseren van getallen van de vorm $n = pq$ met p en q priemgetallen zodat $p-1$ ontbindt in kleine priemfactoren en $q-1$ niet, komt neer op impliciet rekenwerk in de groepen $\mathbb{F}_p^\times$ en $\mathbb{F}_q^\times$. We vermeldden in de les (en in de nota's) dat een variant van deze methode kan worden gebruikt in het geval waarbij $p+1$ splitst in kleine priemfactoren en $q+1$ niet, via impliciet rekenwerk in de quotiëntgroepen

$$\mathbb{F}_{p^2}^\times/\mathbb{F}_p^\times \qquad \text{en} \qquad \mathbb{F}_{q^2}^\times/\mathbb{F}_q^\times.$$

   Werk de details van deze bewering uit. Met andere woorden, beschrijf hoe je zo'n factorisatie-algoritme zou implementeren, waarbij je bijkomend mag aannemen dat $p \equiv q \equiv 3 \bmod 4$. (Deze aanname impliceert dat -1 noch een kwadraat is modulo p, noch modulo q.)

   De aanname vertelt ons dat

$$\frac{\mathbb{Z}_p[x]}{(x^2+1)} \cong \mathbb{F}_{p^2} \qquad \text{en} \qquad \frac{\mathbb{Z}_q[x]}{(x^2+1)} \cong \mathbb{F}_{q^2}. \tag{1}$$

   Onder deze identificaties komen de elementen van $\mathbb{F}_p \subseteq \mathbb{F}_{p^2}$ resp. $\mathbb{F}_q \subseteq \mathbb{F}_{q^2}$ overeen met de uitdrukkingen van de vorm $0x+b$. Het nulelement is in beide gevallen natuurlijk gewoon $0x+0$.

   Uit de Chinese reststelling volgt dat

$$\frac{\mathbb{Z}_n[x]}{(x^2+1)} \cong \frac{\mathbb{Z}_p[x]}{(x^2+1)} \times \frac{\mathbb{Z}_q[x]}{(x^2+1)} \cong \mathbb{F}_{p^2} \times \mathbb{F}_{q^2}.$$

   waarbij het eerste isomorfisme als volgt werkt:

$$\frac{\mathbb{Z}_n[x]}{(x^2+1)} \to \frac{\mathbb{Z}_p[x]}{(x^2+1)} \times \frac{\mathbb{Z}_q[x]}{(x^2+1)} : ax+b \mapsto (ax+b \bmod p, ax+b \bmod q)$$

   (reductie van de coëfficiënten).

Zij nu $\alpha = ax + b \in \mathbb{Z}_n[x]/(x^2+1)$ voor lukraak gekozen $a, b \in \{1, \ldots, n-1\}$ en verifieer dat $\gcd(a, n) = \gcd(b, n) = 1$. Zo niet hebben we onze factor van n reeds beet, in het andere geval hebben we impliciet zeker een element van

$$\mathbb{F}_{p^2}^\times \times \mathbb{F}_{q^2}^\times$$

te pakken. Net als bij Pollard's $(p-1)$-methode kunnen we nu een exponent

$$\gamma = \prod_{\ell \leq M} \ell^{\lfloor \log_\ell n \rfloor} \qquad \text{(product over priemen } \ell \text{ kleiner dan een zekere grens } M\text{)}$$

vinden die een veelvoud is van $p+1$ maar niet van $q+1$. Als we $\alpha^\gamma = a'x + b'$ uitrekenen (net als bij Pollard $p-1$, maar nu via rekenwerk modulo n en modulo x^2+1) komen we in de linkerfactor zeker in $\mathbb{F}_p^\times$ uit omdat

$$\left| \mathbb{F}_{p^2}^\times / \mathbb{F}_p^\times \right| = (p^2-1)/(p-1) = p+1.$$

Wegens de Chinese Reststelling betekent dit dat $p \mid a'$ zodat we hoogst waarschijnlijk p kunnen recupereren als $\gcd(a', n)$. Zo niet betekent dit dat we in de rechterfactor toevallig ook in $\mathbb{F}_q^\times$ terecht kwamen, in welk geval we herproberen met een nieuwe $\alpha = ax + b$.

3. Zij $n, k \geq 2$ en beschouw $nk-1$ vierkante puzzelstukjes gerangschikt in een rechthoek van n bij k vakjes, waarbij het vakje rechtsonder wordt leeg gelaten. Zij $G \subset S_{nk-1}$ de groep van permutaties die twee dergelijke configuraties (dus met het lege vakje rechtsonder) in elkaar omvormen via de gebruikelijke spelregels van een schuifpuzzel.

   Voorbeeld: als $n = 2$ en $k = 3$ kan

1	2	3
4	5	

   via schuiven worden omgevormd tot

1	5	2
4	3	

   en bijgevolg is $(2\ 5\ 3) \in G \subset S_5$.

   (a) Toon aan dat G altijd bevat zit in de alternerende groep A_{nk-1}.

   Beschouw het lege vakje als een extra puzzelstukje met index nk. We bekijken de natuurlijke inclusie

   $$\iota : S_{nk-1} \hookrightarrow S_{nk} : \sigma \mapsto \left(\iota(\sigma) : \begin{cases} i & \mapsto & \sigma(i) & \text{als } 1 \leq i \leq nk-1 \\ nk & \mapsto & nk \end{cases} \right)$$

   die elke permutatie van onze $nk-1$ genummerde puzzelstukjes bekijkt als een permutatie van nk puzzelstukjes die het laatste puzzelstukje vast houdt. Elk element van $\iota(G)$ komt dan tot stand als een samenstelling van een aantal transposities van de vorm $(i\ nk)$. Dit aantal is even omdat het lege vakje uiteindelijk terug op zijn oorspronkelijke plaats moet belanden: het moet even vaak naar links als naar rechts schuiven, en even vaak naar boven als naar beneden. Dus $\iota(G) \subseteq A_{nk}$ wat impliceert dat $G \subseteq A_{nk-1}$, zoals gewenst. Inderdaad, het teken van een permutatie verandert niet onder ι omdat de disjuncte-cykel-schrijfwijze duidelijk niet verandert en omdat het teken hieruit kan worden afgelezen (de permutatie is even als en slechts als het aantal disjuncte cykels van even lengte even is).

   (b) Bewijs dat gelijkheid geldt wanneer $n = 2, k = 3$, dus dat $G = A_5$ in dit geval.
   Hint: vind minstens zeven verschillende elementen van $\mathrm{St}(1) \subset G$.

Voor alle duidelijkheid hebben we het hier over de actie van G op de vijf genummerde puzzelstukjes $\{1,2,3,4,5\}$. Het zou niet moeilijk mogen zijn om zeven elementen in $\mathrm{St}(1)$ te vinden; we lijsten ze hier niet op maar je kreeg id, (2 5 3) en (2 3 5) alvast cadeau in de opgave. Kloksgewijs de puzzelstukjes doorschuiven toont aan dat $|\mathrm{Or}(1)| = 5$. Via de Orbit-Stabilizer Theorem volgt dat

$$|\mathrm{St}(1)| \leq \frac{|G|}{|\mathrm{Or}(1)|} = \frac{|G|}{5}.$$

Als G een echte deelgroep van A_5 zou zijn dan zou $|G| \leq 30$ omwille van de Stelling van Lagrange en dus $|\mathrm{St}(1)| \leq 6$. Onze zeven gevonden elementen tonen dus aan dat $G = A_5$.

(c) Bereken de cycle index van A_5 en bepaal het aantal wezenlijk verschillende 2-bij-3-schuifpuzzels die bekomen kunnen worden door de puzzelstukjes te kleuren met hoogstens $m \geq 1$ kleuren, als functie van m. Hoe verandert deze formule indien we eisen dat minstens twee puzzelstukjes dezelfde kleur moeten hebben?

Herinner dat een permutatie even is als en slechts als het aantal disjuncte cykels van even lengte even is. Voor het berekenen van de cycle index beschouwen we formeel ook cykels van lengte 1 (die we anders niet zouden schrijven). Dit geeft de volgende opdeling van de elementen van A_5:

- de identieke permutatie, die formeel gezien bestaat uit 5 cykels van lengte 1,
- $4! = 24$ vijf-cykels,
- $2 \cdot \binom{5}{3} = 20$ drie-cykels, die formeel gezien nog 2 cykels hebben van lengte 1
- $\frac{1}{2}\binom{5}{2} \cdot \binom{3}{2} = 15$ samenstellingen van twee twee-cykels, waar formeel gezien nog een cykel van lengte 1 aan vast zit.

Dit geeft

$$P_{A_5} = \frac{1}{60}(x_1^5 + 24x_5 + 20x_1^2x_3 + 15x_1x_2^2)$$

zodat Pólyatheorie ons vertelt dat het aantal wezenlijk verschillende manieren om onze puzzelstukjes van hoogstens m kleuren te voorzien gelijk is aan $(m^5+35m^3+24m)/60$.

Voor de tweede vraag passen we de gewogen Stelling van Burnside toe, waarbij we gewicht 1 toekennen aan *goede* kleuringen, i.e., kleuringen v waarbij minstens twee puzzelstukjes eenzelfde kleur hebben. We geven gewicht 0 aan de andere kleuringen. Merk echter op dat voor $\sigma \neq \mathrm{id}$ elke kleuring uit $\mathrm{Fix}(\sigma)$ automatisch goed is. Daarom is de enige term die we moeten herbekijken de term m^5, die moet worden vervangen door

$$\sum_{v \in \mathrm{Fix(id)}} w(v) \;=\; |\text{goede kleuringen in } \mathrm{Fix(id)}|\,.$$

We tellen deze bijdrage als het totaal aantal kleuringen m^5 min het aantal slechte kleuringen, zijnde $m(m-1)(m-2)(m-3)(m-4)$. Dit leidt uiteindelijk tot

$$\frac{m^5 - m(m-1)(m-2)(m-3)(m-4) + 35m^3 + 24m}{60}$$

als antwoord op de tweede vraag.

4. (a) Zij $A \in \{0,1\}^{11\times 11}$ een matrix met de eigenschap dat elke kolom juist 6 eentjes bevat en elk inproduct van twee verschillende kolommen hoogstens 3 is. Toon aan dat A de incidentiematrix is van een symmetrisch 2-(11,6,3)-design.

Hint: beschouw de rijsommen $c_1, c_2, \ldots, c_{11}$ en druk de som van alle inproducten van paren kolommen hierin uit.

We moeten de twee volgende zaken aantonen:

(I) elke *rij* bevat juist 6 eentjes, of met andere woorden $c_1 = c_2 = \ldots = c_{11} = 6$,

(II) voor elk paar kolommen zijn er precies 3 rijen waar de bijhorende entries beide 1 zijn, of met andere woorden elk inproduct van twee kolommen is gelijk aan 3.

Wegens het gegeven dat elke *kolom* juist 6 eentjes bevat zijn er 66 eentjes in totaal, waardoor alvast geldt dat

$$\sum_{i=1}^{11} c_i = 66.$$

We weten ook dat elk paar eentjes op eenzelfde rij juist 1 bijdraagt aan de som van alle inproducten van paren kolommen, waaruit volgt dat deze som gelijk is aan

$$\sum_{i=1}^{11} \binom{c_i}{2} \leq 3\binom{11}{2}. \tag{2}$$

De ongelijkheid geldt omwille van ons gegeven dat elk inproduct van twee kolommen hoogstens 3 is. Het linkerlid kunnen we herschrijven als

$$\sum_{i=1}^{11} \frac{c_i^2 - c_i}{2} = \frac{1}{2}\sum_{i=1}^{11} c_i^2 - \frac{1}{2}\sum_{i=1}^{11} c_i = \frac{1}{2}\sum_{i=1}^{11} c_i^2 - 33$$

waaruit we besluiten dat

$$\sum_{i=1}^{11} c_i^2 \leq 6\binom{11}{2} + 66 = 11 \cdot 36.$$

Nu zouden we ons op Cauchy-Schwartz kunnen beroepen, of meer ad hoc (maar in feite equivalent ermee) kunnen we als volgt te werk gaan. Schrijf $c_i = \lambda_i + 6$, zodat

$$\sum_{i=1}^{11} \lambda_i = 0.$$

Dan is

$$11 \cdot 36 \geq \sum_{i=1}^{11} c_i^2 = \sum_{i=1}^{11} (\lambda_i + 6)^2 = \sum_{i=1}^{11} \lambda_i^2 + 12\sum_{i=1}^{11} \lambda_i + 11 \cdot 36,$$

wat zich herschrijft als

$$0 \geq \sum_{i=1}^{11} \lambda_i^2.$$

Dit kan alleen als alle λ_i's gelijk zijn aan 0, waaruit (I) volgt, en de ongelijkheid in (2) een gelijkheid is, waaruit (II) volgt.

(b) Beschouw de matrix A nu als een element van $\mathbb{F}_2^{11\times 11}$.

(i) Toon aan dat $A^T A = I + J$, waar I de identiteitsmatrix is, en J de matrix met $J_{ij} = 1$ voor alle i, j en concludeer dat $\ker A = \langle (1, \ldots, 1) \rangle$.
Over $\mathbb{Z}$ vinden we net als in de cursus op pp. 22-23 dat

$$A^T A = (r - \lambda)I + \lambda J$$

en dat de eigenwaarden van deze matrix gegeven zijn door $r + (v-1)\lambda$ met multipliciteit 1 en $r - \lambda$ met multipliciteit $v - 1$. In ons geval hebben we de concrete waarden $r = 6$, $\lambda = 3$, $v = 11$. Over $\mathbb{F}_2$ besluiten we dus dat

$$A^T A = I + J,$$

zoals gevraagd. Bovendien zijn de eigenwaarden gegeven door 0 met multipliciteit 1 en 1 met multipliciteit 10, i.h.b. geldt $\dim \ker A^T A = 1$. We kunnen nu besluiten: omdat elke rijsom van A gelijk is aan $6 \equiv 0$ geldt dat $\langle (1, \ldots, 1) \rangle \subseteq \ker A$, en gelijkheid volgt omdat $\dim \ker A \leq \dim \ker A^T A$.

(ii) Beschouw de matrix

$$G = \begin{pmatrix} I \\ P \end{pmatrix}$$

waar I nu de 12×12 identiteitsmatrix voorstelt en P de matrix

$$P = \begin{pmatrix} 0 & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & A & \\ 1 & & & \end{pmatrix}.$$

Zij $\mathcal{C}$ de lineaire $(24, 12)$-code met generatormatrix G^T. Toon aan dat $d_{\mathcal{C}} \geq 8$.

Hint: toon eerst aan dat $w(c) \equiv 0 \bmod 4$ voor elke $c \in \mathcal{C}$, gebruik daarna (i).

We bewijzen eerst de hint en beschouwen de entries als elementen van $\{0, 1\} \subseteq \mathbb{Z}$ in plaats van $\mathbb{F}_2$. De eerste kolom heeft Hamminggewicht 12, de andere hebben Hamminggewicht 8. In beide gevallen is het gewicht dus $0 \bmod 4$. Bovendien is het makkelijk in te zien dat het inproduct van elk paar kolommen even is. We gebruiken nu de volgende vaststelling: voor elk paar vectoren $x_1, x_2 \in \{0, 1\}^n$ van een gegeven lengte n geldt dat

$$w(\overline{x_1 + x_2}) = w(x_1) + w(x_2) - 2\langle x_1, x_2 \rangle,$$

waarbij $\bar{\cdot}$ de reductie modulo 2 naar een element van $\{0, 1\}^n$ voorstelt. Neem nu een lukrake som van m dergelijke vectoren, dan geldt via dezelfde formule dat

$$w(\overline{x_1 + \ldots + x_m}) = w(\overline{x_1 + \ldots + x_{m-1}}) + w(x_m) - 2\langle \overline{x_1 + \ldots + x_{m-1}}, x_m \rangle.$$

Duidelijk is

$$\langle \overline{x_1 + \ldots + x_{m-1}}, x_m \rangle \equiv \langle x_1 + \ldots + x_{m-1}, x_m \rangle = \langle x_1, x_m \rangle + \ldots + \langle x_{m-1}, x_m \rangle \bmod 2$$

wat indien alle inproducten even zijn impliceert dat

$$w(\overline{x_1 + \ldots + x_m}) \equiv w(\overline{x_1 + \ldots + x_{m-1}}) + w(x_m) \bmod 4$$

Omdat elke $c \in \mathcal{C}$ te schrijven is als (de reductie mod 2 van) een som van een aantal kolommen van G volgt de hint per inductie.
Dankzij de hint volstaat het te bewijzen dat er geen codewoord $c \in \mathcal{C}$ bestaat met Hamminggewicht 4. Hiervoor redeneren we op de parity check matrix

$$H = \begin{pmatrix} P & I \end{pmatrix}.$$

Een codewoord met Hamminggewicht 4 komt neer op een som van 4 kolommen van deze matrix die nul is (deze keer redeneren we echt over $\mathbb{F}_2$). We maken een gevalsonderscheid op basis van het aantal kolommen van de vorm

$$\begin{pmatrix} 1 \\ a \end{pmatrix} \quad \text{met } a \text{ een kolom van } A$$

die in deze som betrokken zijn:

- Dit aantal is 0: duidelijk onmogelijk omdat 4 kolommen van I nooit tot nul optellen terwijl 3 kolommen van I nooit tot de eerste kolom van P optellen.
- Dit aantal is 1: om de bovenste 1 weg te werken hebben we alvast de eerste kolom van I nodig. De som van beide kolommen is dan van de vorm

$$\begin{pmatrix} 0 \\ a \end{pmatrix}$$

en heeft bijgevolg precies 6 eentjes. Met twee andere kolommen van I raken deze niet weggewerkt, dus de eerste kolom van P is ook nodig, maar dan zijn er nog 5 eentjes die ook niet raken weggewerkt.
- Dit aantal is 2: de som van beide kolommen is dan van de vorm

$$\begin{pmatrix} 0 \\ a_1 + a_2 \end{pmatrix}$$

en we weten omwille van de design-eigenschappen dat $a_1 + a_2$ precies 6 eentjes heeft, die net als hierboven niet kunnen worden weggewerkt.
- Dit aantal is 3: om de bovenste 1 weg te werken moet de vierde kolom dan de eerste kolom van I zijn. De som van de vier kolommen is dan van de vorm

$$\begin{pmatrix} 0 \\ a_1 + a_2 + a_3 \end{pmatrix}$$

wat niet nul kan zijn omdat de kern van A voortgebracht is door $\langle 1, \ldots, 1 \rangle$ (dus je hebt alle twaalf de kolommen van A nodig om een lineaire afhankelijkheid te vinden).
- Dit aantal is 4: dan is de som van de vorm

$$\begin{pmatrix} 0 \\ a_1 + a_2 + a_3 + a_4 \end{pmatrix}$$

wat om dezelfde reden niet nul kan zijn.

(iii) Beschouw de projectie $\pi : \mathbb{F}_2^{24} \to \mathbb{F}_2^{23}$ op de eerste 23 coordinaten. Toon aan dat de lineaire $(23, 12)$-code $\pi(\mathcal{C})$ een perfecte code is met minimale afstand $d_{\pi(\mathcal{C})} = 7$. Besluit dat $d_{\mathcal{C}} = 8$.

De projectie komt neer op het beschouwen van de matrix G_π bekomen vanaf G door de laatste rij te schrappen: dan is $\pi(\mathcal{C})$ de lineaire $(23, 12)$-code met generatormatrix G_π^T. Duidelijk impliceert $d_{\mathcal{C}} \geq 8$ dat $d_{\pi(\mathcal{C})} \geq 7$. We bekijken nu de Hamminggrens, die zegt dat

$$\sum_{i=0}^{t} \binom{n}{i} (q-1)^i \leq q^{n-k} \tag{3}$$

voor elke lineaire (n, k)-code over $\mathbb{F}_q$ die t fouten kan verbeteren. In ons geval is $q = 2$, $n = 23$, $k = 12$ en omdat $d_{\pi(\mathcal{C})} \geq 7$ weten we dat $t \geq 3$. Omdat

$$\sum_{i=0}^{3} \binom{23}{i} = 2^{23-12}$$

besluiten we dat de Hamminggrens scherp is en dat $t = 3$. Hieruit volgt ook dat $d_{\pi(\mathcal{C})} = 7$ (a priori laat $t = 3$ ook minimumafstand 8 toe, maar uit het bewijs van Stelling 5.30 volgt meteen dat de Hamminggrens in dit geval scherp moest zijn) en dus dat $d_{\mathcal{C}} = 8$.