Vraag 1

Opdracht: maak een computerprogramma dat vraagstukken over lineaire stelsels genereert. (Voorbeelden van alle soorten stelsels moeten voorkomen.)

Hoe ga je te werk?

Antwoord:

- Maak een lijst van de "verschillende" mogelijke lineaire stelsels A van m vergelijkingen in n-onbekenden.
  - $m > n$, $m < n$, $m = n$,
  - strijdig,
  - niet-strijdig, het aantal onafhankelijk oplossingen is gelijk aan $n -$ rang A. (Mogelijkheden voor de rang A: de gehele getallen tussen $1 \leq \min\{m, n\}$)
- Maak voor elk van de mogelijkheden (voor gegeven m, n) een echelon matrix ($m \times (n+1)$-matrix).
- Vermenigvuldig de echelon matrices links met een (random gekozen) rij van elemetaire matrices.

Vraag 2

- Waarom heeft de pariteitscontrole matrix van een 2-foutenverbeterende lineaire code heeft minstens 5 rijen?
- Hoe groot moet de pariteitscontrole matrix van een 2-foutenverbeterende lineaire code zijn om een zinvolle code te genereren?

Antwoord: De afstand tussen 2 woorden in een lineaire 2-fouten vebeterende code moet minstens 5 zijn (twee worden moeten 5 digits verschillen). Een woord dat hoogstens 2 digits verschilt van een code woord verschilt 3 of meer digits van elk ander woord.
Als de matrix hoogstens 4 rijen bevat is de rang van de matrix ≤ 4, elke 5 kolommen zijn lineair afhankelijk. Alle stellen van 4 kolommen, dus ook de eerste 4 kolommen, moeten lineair onafhankelijk zijn anders is er een woord dat 4 of minder digits verschilt van het nulwoord, de code is dan niet 2-fouten verbeterend. Die eerste vier kolommen vormen een basis voor de kolommen ruimte, elke volgende kolom is dan een lineaire combinatie van de eerste vier, en het moet de combinatie $K_1 + K_2 + K_3 + K_4$ zijn (anders zijn er 4 of minder lineair afhankelijke kolommen). De matrix kan maar 5 kolommen hebben vermits alle volgende kolommen moeten gelijk zijn, en dit kan niet als de code 2-fouten verbeterend is.
Als de pariteits controle matrix een 4×5 matrix is, is er maar 1 niet nul code woord, dat is niet zinvol.

Hoeveel code woorden moet een praktisch zinvolle code hebben. Hoe groter het geeiste aantal code woorden hoe meer rijen de matrix moet hebben om te garanderen dat elk stel van 4 kolommen lineair onafhankelijk is.

Vraag 3

Zij $(b_1, f(b_1)), \ldots, (b_n, f(b_n))$ de sleutels van n personen in een Shamir secret sharing systeem waarbij 3 sleutels nodig zijn om de geheime code te bekomen. Toon aan dat voor elk stel $(b_{i_1}, f(b_{i_1})), (b_{i_2}, f(b_{i_2})), (b_{i_3}, f(b_{i_3}))$ van drie verschillende sleutels de vectoren

$$\begin{pmatrix} 1 \\ b_{i_1} \\ b_{i_1}^2 \end{pmatrix}, \begin{pmatrix} 1 \\ b_{i_2} \\ b_{i_2}^2 \end{pmatrix}, \begin{pmatrix} 1 \\ b_{i_3} \\ b_{i_3}^2 \end{pmatrix},$$

lineair onafhankelijk zijn over $\mathbb{R}$.

Antwoord:
Bereken de determinant van de matrix bestaand uit de drie kolommen. De determinant is $\pm(b_{i_1} - b_{i_2})(b_{i_1} - b_{i_3})(b_{i_2} - b_{i_3})$. Deze is nul als en slechts als er twee gelijke kolommen zijn. Dus drie verschillende sleutels geven 3 lineair onafhankelijke voorwaarden (de kolommen zijn lineair onafhankelijk dan en slechts dan als de determinant van de matrix ongelijk is aan nul).

Vraag 4

- Is de Markov eigenschap een eigenschap van de matrix of een eigenschap van de lineaire afbeelding die door de matrix bepaald wordt?
- Anders geformuleerd: als A de matrixvoorstelling is van een lineaire operator f en A is een Markov matrix, is dan elke andere matrixvoorstelling van f ook een Markov matrix?

Antwoord: Een 2×2-markov matrix met slechts 1 eigenwaarde met absolute waarde gelijk aan 1, heeft twee verschillende eigenwaarden en is dus diagonaliseerbaar. De kolom in de diagonaal matrix met de eigenwaarde λ met $|\lambda| \neq 1$ voldoet niet aan de Markov voorwaarde (som van de elementen in een kolom is 1). Dus de Markov eigenschap is geen eigenschap van de lineaire afbeelding.

Vraag 5

Toon aan dat als A een Markov matrix, A^n een Markov matrix is voor alle $n \in \mathbb{N}$.

Als A een (inverteerbare) Markov matrix is, is A^{-1} dan ook een Markov matrix?

Antwoord:
De eigenschap dat de som van de elementen in een kolom gelijk is aan 1, kan men verifiëren door de matrix links te vermenigvuldigen met de rij $(1, \ldots, 1)$. Nu is als A Markov is

$$(1, \ldots, 1)A^n = ((1, \ldots, 1)A)A^{n-1} = (1, \ldots, 1)A^{n-1} = \cdots = (1, \ldots, 1)A = (1, \ldots, 1).$$

De eigenschap dat de elementen in de matrix getallen moeten zijn tussen nul en 1 volgt uit het feit dat in een product van twee zulke matrices alle componenten positief zijn vermits

ze gelijk zijn aan de som van positieve elementen. De som van positieve elementen kan enkel gelijk zijn aan 1 als die elementen ≤ 1.

De Markov matrix $\begin{pmatrix} \frac{1}{2} & 0 \\ \frac{1}{2} & 1 \end{pmatrix}$ heeft als een inverse $\begin{pmatrix} 2 & 0 \\ -1 & 1 \end{pmatrix}$. Dit is geen Markov matrix. (Merk op dat de eigenschap dat de som van de elementen in een kolom gelijk is aan 1 wel geldt voor A^{-1}.)