1. *Van-e olyan $U \leq \mathbb{F}_2^n = V$, hogy*
a) $U = U^\perp$;
b) $V = U \oplus U^\perp$?

Megoldás: a) Mivel $\dim U^\perp = n - \dim U$, páratlan n-re nem létezhet ilyen altér. Ha n páros, akkor viszont az $(1,1,0,0,\ldots)$, $(0,0,1,1,0,0,\ldots),\ldots,$ $(0,0,\ldots,0,0,1,1)$ vektorok által generált U altérre igaz, hogy $\dim U = \frac{n}{2}$, és U merőleges önmagára, ezért $U^\perp \geq U$, és a dimenziók egyenlősége miatt ebből $U^\perp = U$ következik.

b) A $\dim U^\perp = n - \dim U$ összefüggés miatt elég olyan U-t találni, amelyre $U \cap U^\perp = \{\mathbf{0}\}$. Ezt pedig bármely olyan egydimenziós altér kielégíti, amelynek generátoreleme páratlan sok 1-est tartalmaz. Tehát ilyen U minden $n \geq 2$ esetén van a triviális altereken kívül is.

2. *Bizonyítsuk be, hogy $V = \mathbb{F}_3^2$-ben minden U altérre $V = U \oplus U^\perp$, de $\mathbb{F}_3^3$-ben ez nem igaz!*

Megoldás: A $\{\mathbf{0}\}$ altérre és a teljes vektortérre nyilván igaz az állítás. Ezenkívül csak 1-dimenziós alterek vannak $\mathbb{F}_3^2$-ben, amelyekről az 1.b) feladat megoldásához hasonlóan csak azt kell belátni, hogy a generátoreleme nem merőleges önmagára. Ha a generátorelem $\mathbf{0} \neq (a,b) \in \mathbb{F}_3^2$, akkor az önmagával vett skalárszorzata $a^2 + b^2$ csak 1 vagy 2 lehet, tehát az általa generált U altérre $V = U \oplus U^\perp$. $\mathbb{F}_3^3$-ban viszont van olyan nemnulla vektor, amelyik merőleges önmagára, például $(1,1,1)$ ilyen.

3. *Legyen V vektortér egy $\langle\ ,\ \rangle$ bilineáris függvénnyel, és legyen $U \leq V$. Bizonyítsuk be, hogy ha U-nak van olyan ortogonális bázisa, amelynek semelyik eleme sem merőleges önmagára, akkor $V = U \oplus U^\perp$.*

Megoldás: $\dim U^\perp = \dim V - \dim U$ miatt elég azt belátni, hogy $U \cap U^\perp = \{\mathbf{0}\}$. Egy $\mathbf{u}$ vektor akkor és csak akkor van $U^\perp$-ben, ha merőleges az U minden báziselemére. Viszont az ortonomált bázis elemeivel való skalárszorzatok éppen az $\mathbf{u}$ előállításában az egyes báziselemek együtthatóit adják. Tehát egy U-beli elem akkor és csak akkor merőleges U-ra, ha az előállításában minden együttható 0, azaz a vektor a nullvektor.

4. *Ellenőrizzük, hogy a Hamming-kód perfekt!*

Megoldás: Azt kell belátnunk, hogy $|C| \cdot \sum_{s=0}^{t} \binom{n}{s}(q-1)^s = q^n$, ahol C a kódszavak halmaza, q az abc elemszáma, n a kódhossz, és $2t+1$ a kódtávolság. A Hamming-kódnál $|C| = 2^{n-m}$, $n = 2^m - 1$, $q = 2$ és $t = 1$. Tehát az egyenlőség bal oldala $2^{n-m} \cdot (1+n) = 2^{n-m} \cdot 2^m = 2^n$, ezért a Hamming-kód perfekt.

5. *Határozzuk meg az Hadamard-kód duálisának dimenzióját, kódhosszát, kódtávolságát!*

Megoldás: A duális kódhossza megegyezik az Hadamard-kód kódhosszával 2^m-mel, dimenziója pedig az Hadamard-kód dimenziójának kiegészítője, $2^m - m - 1$. Az Hadamard-kód G generátormátrixát megkaphatjuk, ha felírjuk $\mathbb{F}_2^m$ vektorait sorvektorokként egy mátrixba, aztán ezt a mátrixot kiegészítjük egy csupa 1-esből álló oszloppal (ugyanis az $\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 + \beta$ kiértékeléseit úgy kaphatjuk meg, hogy az $[x_1 \quad x_2 \quad x_3 \quad 1]$ sorvektort megszorozzuk az $[\alpha_1 \quad \alpha_2 \quad \alpha_3 \quad \beta]^T$ oszlopvektorral). A duálisban azok a 2^m hosszú vektorok vannak, amelyek a G oszlopaira merőlegesek, azaz amelyek megadják a G sorai $\mathbf{0}$ értékű lineáris kombinációinak együtthatóit. A kódtávolság az a legkisebb szám, ahány különböző sor összege a G-ben $\mathbf{0}$ lehet. Semelyik sor nem 0, mert mindegyik sor végén van egy 1-es, és két sor összege nem lehet 0, mert akkor a két sor egyenlő lenne. Három sor összege sem lehet 0, mert az utolsó koordináta 1, négy sor összege viszont már lehet 0. Így a kódtávolság 4.

6. *$m = 3$ paraméterű Hadamard-kóddal elkódolva érkezett ez az üzenet:*
8520 4C2F 3454 3C38 10C3 2434 F055 6855 34B0 A8A2
(a rövidség kedvéért a bináris üzenetet átírtuk hexadecimálissá). Az angol abc huszonhat betűjét ötjegyű bináris számokkal kódoltuk el eredetileg, 00001-től 11010-ig, a szóköz a 00000, majd négyes csoportokra osztva alkalmaztuk rá az Hadamard-kódot (a vektortér elemeit is a bináris számok sorrendjében, 000-tól 111-ig helyettesítettük be). Fejtsük meg az üzenetet! (Kettőnél több hiba egyik

kódszóba se csúszott; ahol kettő van, írjuk fel a lehetséges javításokat, és a szöveg értelme szerint találjuk ki, hogy mi a megfejtés!)

Megoldás: Az 5. feladatban leírt G generátormátrix az $m = 3$ eseben:

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}.$$

Ezt ráalkalmazva $0 = 0000$-tól $F = 1111$-ig a legföljebb négyjegyű bináris számokra mint 4-dimenziós $\mathbb{F}_2$ fölötti vektorokra, a következő kódolást kapjuk (az eredmény szintén 16-os számrendszerbe átírva):

$0 \to 00$	$4 \to 33$	$8 \to 0F$	$C \to 3C$
$1 \to FF$	$5 \to CC$	$9 \to F0$	$D \to C3$
$2 \to 55$	$6 \to 66$	$A \to 5A$	$E \to 69$
$3 \to AA$	$7 \to 99$	$B \to A5$	$F \to 96$

Ha a kapott üzenetet 8 bites szakaszokra, azaz kétjegyű hexadecimális számokra bontjuk, akkor egy kivételével találunk ezekhez egy bit eltérésű kódszót: ezeknél az egyik számjegy nem is szerepel kódszóban $(1, 2, 4, 7, 8, B, D, E)$, és a másik számjegyhez csak kétféle pár tartozhat, amelyek közül az egyik tér el csupán egy bitben az az elrontott kódszó másik jegyétől. A 24-től 2 távolságra levő kódszavak $A5$, 66, 00 és $3C$. Tehát a javított üzenet: A500 CC0F 3C55 3C3C 00C3 {A5, 66, 00 vagy 3C}3C F055 6955 3CF0 AAAA. A kódtáblázatból visszakeresve az üzenet hexadecimálisan:

B 0 5 8 C 2 C C 0 D {B, 6, 0 vagy C} C 9 2 E 2 C 9 3 3

és ebből binárisan:

1011000001011000110000101100110000001101

{1011,0110,0000,1100 }1100100100101110001011001001001100 11.

Ezt ötbites részekre tördelve, decimálisan:

22,1,12,12,5,19,0,13,{23,13,1,25},18,9,14,5,18,9,19,

az ilyen sorszámú betűk: VALLES M{WMAY}RINERIS,

és ebből a megfejtés: Valles Marineris.

7. *Adjunk meg ortogonális, illetve ortonomált bázist az* $\mathbb{R}^4$ $(1, 2, -1, 0)$, $(2, 1, 0, 1)$ *és* $(1, -1, 1, -1)$ *vektorok által generált alterében!*

Megoldás: Cseréljük ki a $\mathbf{v}_1 = (1, 2, -1, 0)$, $\mathbf{v}_2 = (2, 1, 0, 1)$ és $\mathbf{v}_3 = (1, -1, 1, -1)$ vektorokat ortogonálisakra a Gram–Schmidt-módszerrel.

$$\mathbf{v}_1 = (1, 2, -1, 0) =: \mathbf{w}_1$$

$$\mathbf{v}_2 - \frac{\mathbf{v}_2\mathbf{w}_1}{\mathbf{w}_1\mathbf{w}_1}\mathbf{w}_1 = (2, 1, 0, 1) - \frac{4}{6}(1, 2, -1, 0) = (\frac{4}{3}, -\frac{1}{3}, \frac{2}{3}, 1) \parallel (4, -1, 2, 3) =: \mathbf{w}_2$$

$$\mathbf{v}_3 - \frac{\mathbf{v}_3\mathbf{w}_1}{\mathbf{w}_1\mathbf{w}_1}\mathbf{w}_1 - \frac{\mathbf{v}_3\mathbf{w}_2}{\mathbf{w}_2\mathbf{w}_2}\mathbf{w}_2 = (1, -1, 1, -1) - \frac{-2}{6}(1, 2, -1, 0) - \frac{4}{30}(4, -1, 2, 3) =$$

$$= (\frac{4}{5}, -\frac{1}{5}, \frac{2}{5}, -\frac{7}{5}) \parallel (4, -1, 2, -7) =: \mathbf{w}_3.$$

Ha ezeket a vektorokat elosztjuk a hosszukkal, akkor ortonormált rendszert kapunk: $\frac{1}{\sqrt{6}}(1, 2, -1, 0)$, $\frac{1}{\sqrt{30}}(4, -1, 2, 3)$, $\frac{1}{\sqrt{70}}(4, -1, 2, -7)$

8. *Legyen $V = \mathbb{R}^5$ a szokásos skalárszorzattal, és U azon vektorok halmaza, amelyekben az első két koordináta összege egyenlő az utolsó két koordináta összegével.*

a) Adjunk meg U-ban egy ortonormált bázist!
b) Határozzuk meg $U^\perp$ elemeit!
c) Írjuk fel az (1,0,0,0,0) vektort egy U-beli és egy $U^\perp$-beli vektor összegeként!

Megoldás: b) Az $U = \{(x_1, x_2, x_3, x_4, x_5) \in \mathbb{R}^5 \,|\, x_1 + x_2 - x_4 - x_5 = 0\}$ altér éppen a $\mathbf{v} = (1, 1, 0, -1, -1)$ vektorra merőleges vektorokból áll, azaz $U = \langle \mathbf{v} \rangle^\perp$, és ebből $(U^\perp) = (\langle \mathbf{v} \rangle^\perp)^\perp = \langle \mathbf{v} \rangle$.

c) Az $U^\perp$-re való vetületet könnyebb kiszámolni: $\mathbf{e}_1 = (1, 0, 0, 0, 0)$ vetülete $\frac{\mathbf{e}_1\mathbf{v}}{\mathbf{v}\mathbf{v}}\mathbf{v} = \frac{1}{4}\mathbf{v} = (\frac{1}{4}, \frac{1}{4}, 0, -\frac{1}{4}, -\frac{1}{4})$, és ebből a felbontás $e_1 = (1, 0, 0, 0, 0) = (\frac{3}{4}, -\frac{1}{4}, 0, \frac{1}{4}, \frac{1}{4}) + (\frac{1}{4}, \frac{1}{4}, 0, -\frac{1}{4}, -\frac{1}{4})$.

a) Gram–Schmidt-ortogonalizációval készítsünk ortogonális bázist a $\mathbf{v}, \mathbf{e}_1, \ldots, \mathbf{e}_n$ generátorrendszerből.

$$\mathbf{v} = (1, 1, 0, -1, -1) =: \mathbf{w}_1$$

$$\begin{aligned}\mathbf{e}_1 - \frac{\mathbf{e}_1\mathbf{w}_1}{\mathbf{w}_1\mathbf{w}_1}\mathbf{w}_1 =& (1, 0, 0, 0, 0) - \frac{1}{4}(1, 1, 0, -1, -1) = \\ =& \left(\frac{3}{4}, -\frac{1}{4}, 0, \frac{1}{4}, \frac{1}{4}\right) \;||\; (3, -1, 0, 1, 1) =: \mathbf{w}_2\end{aligned}$$

$$\begin{aligned}\mathbf{e}_2 - \frac{\mathbf{e}_2\mathbf{w}_1}{\mathbf{w}_1\mathbf{w}_1}\mathbf{w}_1 - \frac{\mathbf{e}_2\mathbf{w}_2}{\mathbf{w}_2\mathbf{w}_2}\mathbf{w}_1 =& (0, 1, 0, 0, 0) - \frac{1}{4}(1, 1, 0, -1, -1) - \frac{-1}{12}(3, -1, 0, 1, 1) = \\ =& \left(0, \frac{2}{3}, 0, \frac{1}{3}, \frac{1}{3}\right) \;||\; (0, 2, 0, 1, 1) =: \mathbf{w}_3\end{aligned}$$

$$\mathbf{e}_3 - \sum_{i=1}^{3} \frac{\mathbf{e}_3\mathbf{w}_i}{\mathbf{w}_i\mathbf{w}_i}\mathbf{w}_i = (0, 0, 1, 0, 0) - 0\mathbf{w}_1 - 0\mathbf{w}_2 - 0\mathbf{w}_3 = (0, 0, 1, 0, 0) =: \mathbf{w}_4$$

$$\begin{aligned}\mathbf{e}_4 - \sum_{i=1}^{4} \frac{\mathbf{e}_3\mathbf{w}_i}{\mathbf{w}_i\mathbf{w}_i}\mathbf{w}_i =& (0, 0, 0, 1, 0) - \frac{-1}{4}(1, 1, 0, -1, -1) - \frac{1}{12}(3, -1, 0, 1, 1) - \frac{1}{6}(0, 2, 0, 1, 1) - \mathbf{0} \\ =& \left(0, 0, 0, \frac{1}{2}, -\frac{1}{2}\right) \;||\; (0, 0, 0, 1, -1) =: \mathbf{w}_5\end{aligned}$$

$$\begin{aligned}\mathbf{e}_5 - \sum_{i=1}^{5} \frac{\mathbf{e}_3\mathbf{w}_i}{\mathbf{w}_i\mathbf{w}_i}\mathbf{w}_i =& (0, 0, 0, 0, 1) - \frac{-1}{4}(1, 1, 0, -1, -1) - \frac{1}{12}(3, -1, 0, 1, 1) \\ & -\frac{1}{6}(0, 2, 0, 1, 1) - \mathbf{0} - \frac{-1}{2}(0, 0, 0, 1, -1) = \mathbf{0}\end{aligned}$$

Tehát $\{\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3, \mathbf{w}_4, \mathbf{w}_5\}$ ortogonális bázisa V-nek, s mivel az első báziselem $U^\perp$-t generálja, U bázisa $\{\mathbf{w}_2, \mathbf{w}_3, \mathbf{w}_4, \mathbf{w}_5\}$, U ortonormált bázisa pedig $\{\frac{1}{\sqrt{12}}\mathbf{w}_2, \frac{1}{\sqrt{6}}\mathbf{w}_3, \mathbf{w}_4, \frac{1}{\sqrt{2}}\mathbf{w}_5\}$.

9. *Az alábbi mátrixok közül melyek határoznak meg szimmetrikus bilineáris, illetve hermitikus bilineáris függvényt? Ezeket hozzuk diagonális alakra, és állapítsuk meg, milyen definitek! A valósakhoz adjunk is meg ortogonális bázist!*

$$A = \begin{bmatrix} 0 & 1 & 0 \\ -1 & 2 & 1 \\ 0 & -1 & 1 \end{bmatrix} \qquad B = \begin{bmatrix} 2 & 1 & 0 \\ 1 & 4 & 1 \\ 0 & 1 & 2 \end{bmatrix} \qquad C = \begin{bmatrix} -1 & 2+i \\ 2-i & 2 \end{bmatrix}$$

$$D = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \qquad E = \begin{bmatrix} 0 & 1 & 2 \\ 1 & -1 & 0 \\ 2 & 0 & 1 \end{bmatrix} \qquad F = \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}$$

Megoldás: B, D, E szimmetrikus bilineáris, C hermitikus bilineáris függvényt ad meg. E-ről és C-ről diagonális alakra hozás nélkül is látjuk, hogy indefinit, mert az átlójában pozitív és negatív szám is van (azaz $\mathbf{e}_2^* E \mathbf{e}_2 < 0$, és $\mathbf{e}_3^* E \mathbf{e}_3 > 0$, illetve $\mathbf{e}_1^* C \mathbf{e}_1 < 0$ és $\mathbf{e}_2^* C \mathbf{e}_2 > 0$). A többiek jellegét a diagonális alakjukból tudjuk eldönteni.

$$B = \begin{bmatrix} 2 & 1 & 0 \\ 1 & 4 & 1 \\ 0 & 1 & 2 \end{bmatrix} \mapsto \begin{bmatrix} 2 & 1 & 0 \\ 0 & \frac{7}{2} & 1 \\ 0 & 1 & 2 \end{bmatrix} \mapsto \begin{bmatrix} 2 & 0 & 0 \\ 0 & \frac{7}{2} & 1 \\ 0 & 1 & 2 \end{bmatrix} \mapsto \begin{bmatrix} 2 & 0 & 0 \\ 0 & \frac{7}{2} & 1 \\ 0 & 0 & \frac{12}{7} \end{bmatrix} \mapsto \begin{bmatrix} 2 & 0 & 0 \\ 0 & \frac{7}{2} & 0 \\ 0 & 0 & \frac{12}{7} \end{bmatrix}$$

Tehát B pozitív definit, és az áttérés mátrixát megkaphatjuk I-ből, ha végrehajtjuk rajta ugyanazokat az oszlopműveleteket, mint B-n.

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 & -\frac{1}{2} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 & -\frac{1}{2} & \frac{1}{7} \\ 0 & 1 & -\frac{2}{7} \\ 0 & 0 & 1 \end{bmatrix}$$

Tehát az új bázis $\{(1,0,0),\ (-\frac{1}{2},1,0),\ (\frac{1}{7},-\frac{2}{7},1)\}$.

$$D = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix},$$

tehát a D-hez tartozó bilineáris függvény pozitív szemidefinit, és a diagonális alakhoz tartozó bázis $\{(1,0,0),\ (-1,1,0),\ (-1,0,1)\}$.

$$E = \begin{bmatrix} 0 & 1 & 2 \\ 1 & -1 & 0 \\ 2 & 0 & 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 & 0 & 2 \\ 1 & -1 & 0 \\ 2 & 0 & 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 & 0 & 2 \\ 0 & -1 & 0 \\ 2 & 0 & 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 & 0 & 2 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix},$$

tehát a E-hez tartozó bilineáris függvény indefinit, a diagonális alakhoz tartozó bázis pedig $\{(1,1,0),\ (0,1,0),\ (-2,0,1)\}$.

$$C = \begin{bmatrix} -1 & 2+i \\ 2-i & 2 \end{bmatrix} \mapsto \begin{bmatrix} -1 & 2+i \\ 0 & 7 \end{bmatrix} \mapsto \begin{bmatrix} -1 & 0 \\ 0 & 7 \end{bmatrix}$$

indefinit.

10. *Adjunk példát olyan komplex (és nem valós) önadjungált mátrixra, amely negatív szemidefinit, és nem negatív definit!*

Megoldás: Egy alkalmas diagonális alakból, pl. $\begin{bmatrix} -1 & 0 \\ 0 & 0 \end{bmatrix}$-ból szimultán sor- és oszlopművelettel létrehozhatunk ilyet. Mondjuk, az első sor i-szeresét adjuk hozzá a másodikhoz, aztán az első oszlop $-i$-szeresét a második oszlophoz: $\begin{bmatrix} -1 & i \\ -i & -1 \end{bmatrix}$.

11. *Bizonyítsuk be, hogy ha egy $\langle\ ,\ \rangle$ valós szimmetrikus vagy komplex hermitikus bilineáris függvény nem pozitív vagy negatív definit, akkor van olyan $\mathbf{v} \neq \mathbf{0}$ vektor, amelyre $\langle \mathbf{v}, \mathbf{v} \rangle = 0$.*

Megoldás: Legyen $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ a $\langle\ ,\ \rangle$-re nézve ortogonális bázis. Ha van i, hogy $\langle \mathbf{b}_i, \mathbf{b}_i \rangle = 0$, akkor kész vagyunk. Ha nincs, akkor a feltétel miatt van i, j, hogy $\langle \mathbf{b}_i, \mathbf{b}_i \rangle = c > 0$, és $\langle \mathbf{b}_j, \mathbf{b}_j \rangle = -d < 0$. Ekkor $\mathbf{v} = \sqrt{d}\mathbf{b}_i + \sqrt{c}\mathbf{b}_j$-re $\langle \mathbf{v}, \mathbf{v} \rangle = d\langle \mathbf{b}_i, \mathbf{b}_i \rangle + c\langle \mathbf{b}_j, \mathbf{b}_j \rangle = dc - cd = 0$, és $\mathbf{v} \neq \mathbf{0}$, mert $\mathbf{b}_i$ és $\mathbf{b}_j$ függetlenek.