Láttuk, hogy a 2^m hosszú Hadamard-kód $\left[\dfrac{2^{m-1}-1}{2}\right] = (2^{m-2}-1)$-hibajavító. Pl. a Mariner 9 Mars-szonda (1971) $m = 5$ paraméterű Hadamard-kódot használt: $n = 32$, $k = 6$, $d = 16 \Rightarrow 7$-hibajavító, kódsebessége $\frac{6}{32} \approx \frac{1}{5}$. Az ugyanilyen kódtávolságú ismétlőkód ($n = 16$, $k = 1$, $d = 16$) 3-szor lassabb.

Hadamard-kód fele

Csak $\alpha_1 x_1 + \ldots + \alpha_m x_m$ alakú (tehát lineáris) függvényeket használunk. Ekkor elég a $2^m - 1$ darab $\neq \mathbf{0}$ vektoron nézni az értéket, mert $\mathbf{0} \mapsto \mathbf{0}$ mindegyikre igaz. Erre $k = m$, $n = 2^m - 1$, $d = 2^{m-1}$, mint az előbb.

Def. duális kód: $U \leq K^n$ duálisa $U^\perp$.

Hamming-kód: a fél Hadamard-kód duálisa.

kódhossz: $n = 2^m - 1$
dimenzió: $k = 2^m - 1 - m$

Állítás. A Hamming-kód kódtávolsága 3, tehát a Hamming-kód 1-hibajavító kód.

Bizonyítás. Legyen $\mathbb{F}_2^m \setminus \{\mathbf{0}\} = \{\mathbf{v}_1, \ldots, \mathbf{v}_{2^m-1}\}$, és

$$G = \begin{bmatrix} \mathbf{v}_1 \\ -- \\ \vdots \\ -- \\ \mathbf{v}_{2^m-1} \end{bmatrix} = [\,\mathbf{u}_1 \quad | \quad \cdots \quad | \quad \mathbf{u}_m\,]$$

(a $\mathbf{v}_i$-ket sorvektorokként írva). Ekkor $\mathbf{u}_j \in U\ \forall j$, mert $\mathbf{u}_j$ a j. komponensre való vetítésnek mint lineáris függvénynek a behelyettesítési vektora (kódszó a fél-Hadamard kódban).

Ha $\mathbf{a} \in U^\perp$, akkor

$$\mathbf{a}^T G = \left[a_1 | \cdots | a_{2^m-1}\right] \begin{bmatrix} \mathbf{v}_1 \\ -- \\ \vdots \\ -- \\ \mathbf{v}_{2^m-1} \end{bmatrix} = \sum a_i \mathbf{v}_i \text{ és}$$

$$\mathbf{a}^T G = [\mathbf{a}^T] \cdot \left[\mathbf{u}_1 \mid \cdots \mid \mathbf{u}_m\right] = [\mathbf{a}^T\mathbf{u}_1 | \cdots | \mathbf{a}^T\mathbf{u}_m] = [0| \cdots |0] = \mathbf{0}$$

Tehát $\mathbf{a} \in U^\perp \Rightarrow \sum a_i \mathbf{v}_i = \mathbf{0}$.

$U^\perp$-ben

nincs 1 súlyú vektor, mert $\mathbf{v}_i \neq \mathbf{0}\ \forall i$;
nincs 2 súlyú vektor, mert $i \neq j$-re nem lehet $\mathbf{v}_i + \mathbf{v}_j = \mathbf{0}$, ui. akkor $\mathbf{v}_i = \mathbf{v}_j$ lenne;
van 3 súlyú vektor, mert $i \neq j$-re $\mathbf{v}_i + \mathbf{v}_j = \mathbf{v}_k$ valamely k-ra, és akkor $\mathbf{v}_i + \mathbf{v}_j + \mathbf{v}_k = \mathbf{0}$.

Hamming-korlát

Legyen C nem feltétlenül lineáris kód a q elemű abc fölött. Tegyük fel, hogy C szavainak távolsága $\geq 2t + 1$, a kódszavainak hossza pedig n. Ekkor

$$|C| \sum_{s=0}^{t} \binom{n}{s} (q-1)^s \leq q^n.$$

Def. perfekt kód: amelyre a Hamming-korlátban egyenlőség áll.

Pl.: A Hamming-kódok perfektek (ld. 3. feladatsorban).

□

Euklideszi terek

Def. valós euklideszi tér:
$V_{\mathbb{R}}$, $\langle\ ,\ \rangle$ szimmetrikus bilineáris függvény,
és $\langle \mathbf{v}, \mathbf{v} \rangle > 0$, ha $\mathbf{v} \neq \mathbf{0}$ (azaz $\langle\ ,\ \rangle$ **pozitív definit**)

Jelölés: $|\mathbf{v}| = \sqrt{\langle \mathbf{v}, \mathbf{v} \rangle}$.

Tétel. (**Gram–Schmidt-féle ortogonalizáció**) Egy valós euklideszi térben $\forall\ \mathbf{b}_1, \ldots, \mathbf{b}_k$ független rendszerhez $\exists\ \mathbf{e}_1, \ldots, \mathbf{e}_k$ ortonormált rendszer, amely ugyanazt az alteret generálja, sőt, ugyanazt az altérláncot generálja: $\langle \mathbf{b}_1, \ldots, \mathbf{b}_i \rangle_V = \langle \mathbf{e}_1, \ldots, \mathbf{e}_i \rangle_V\ \forall i$.

Bizonyítás. Legyen $\mathbf{e}_1 = \dfrac{\mathbf{b}_1}{|\mathbf{b}_1|}$. Ha i-ig megvan:

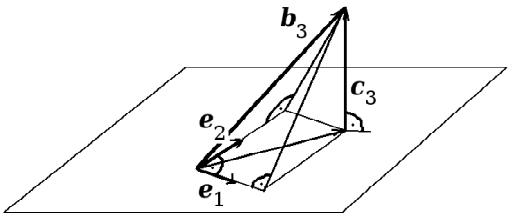
$$\mathbf{c}_{i+1} = \mathbf{b}_{i+1} - \sum_{j=1}^{i} \langle \mathbf{b}_{i+1}, \mathbf{e}_j \rangle\, \mathbf{e}_j$$

$\mathbf{c}_{i+1} \neq \mathbf{0}$, mivel a szumma $\langle \mathbf{e}_1, \ldots, \mathbf{e}_i \rangle_V$-ben van, és ez $= \langle \mathbf{b}_1, \ldots, \mathbf{b}_i \rangle_V$ az indukciós feltevés szerint,

$\mathbf{c}_{i+1} \in \langle \mathbf{e}_1, \ldots, \mathbf{e}_i, \mathbf{b}_{i+1} \rangle = \langle \mathbf{b}_1, \ldots, \mathbf{b}_i, \mathbf{b}_{i+1} \rangle$, és

$\langle \mathbf{c}_{i+1}, \mathbf{e}_j \rangle = \langle \mathbf{b}_{i+1}, \mathbf{e}_j \rangle - \langle \mathbf{b}_{i+1}, \mathbf{e}_j \rangle = 0$, ha $j \leq i$.

Ekkor $\mathbf{e}_{i+1} = \dfrac{\mathbf{c}_{i+1}}{|\mathbf{c}_{i+1}|}$-re az előbbiek miatt teljesülnek az előírt feltételek.



Megjegyzés. Lehet először csak ortogonális rendszert gyártani, és azután normálni:
ha $\mathbf{u}_1, \ldots, \mathbf{u}_i$ ortogonális, és $\langle \mathbf{u}_1, \ldots, \mathbf{u}_i \rangle = \langle \mathbf{b}_1, \ldots, \mathbf{b}_i \rangle$, akkor

$$\mathbf{u}_{i+1} = \mathbf{b}_{i+1} - \sum_{j=1}^{i} \frac{\langle \mathbf{b}_{i+1}, \mathbf{u}_j \rangle}{\langle \mathbf{u}_j, \mathbf{u}_j \rangle} \mathbf{u}_j,$$

(vagy ennek egy tetszőleges $\neq 0$ skalárszorosa).

Ha a $\{\mathbf{b}_1, \ldots, \mathbf{b}_k\}$ rendszer nem független, akkor néhány lépésben $\mathbf{0}$-t kapunk, de a $\mathbf{0}$-kat egyszerűen kihagyjuk, és úgy folytatjuk tovább az algoritmust. Tehát nem kell előre bázist keresnünk az altérben, elég egy generátorrendszerrel indulni.

Pl.: Adjunk ortonormált bázist az $U = \langle (1,0,-1,1),(0,2,1,-1),(1,1,0,0)\rangle \leq \mathbb{R}^4$ altérben!

Megoldás:

$$\begin{aligned}
\mathbf{u}_1 =&(1,0,-1,1)\\
\mathbf{u}_2 =&(0,2,1,-1) - \tfrac{-2}{3}(1,0,-1,1) = (\tfrac{2}{3},2,\tfrac{1}{3},-\tfrac{1}{3}) \;||\; (2,6,1,-1) =: \mathbf{u}_2'\\
\mathbf{u}_3 =&(1,1,0,0) - \tfrac{1}{3}(1,0,-1,1) - \tfrac{8}{42}(2,6,1,-1) =\\
=&(1,1,0,0) + (-\tfrac{1}{3},0,\tfrac{1}{3},-\tfrac{1}{3}) + (-\tfrac{8}{21},-\tfrac{8}{7},-\tfrac{4}{21},\tfrac{4}{21}) =\\
=&(\tfrac{6}{21},-\tfrac{1}{7},\tfrac{3}{21},-\tfrac{3}{21}) = (\tfrac{2}{7},-\tfrac{1}{7},\tfrac{1}{7},-\tfrac{1}{7}) \;||\; (2,-1,1,-1) =: \mathbf{u}_3'
\end{aligned}$$

Tehát

$$\{(1,0,-1,1),\ (2,6,1,-1),\ (2,-1,1,-1)\}$$

ortogonális bázis U-ban, és

$$\left\{\tfrac{1}{\sqrt{3}}(1,0,-1,1),\ \tfrac{1}{\sqrt{42}}(2,6,1,-1),\ \tfrac{1}{\sqrt{7}}(2,-1,1,-1)\right\}$$

ortonormált.

Következmény. Minden n-dimenziós valós euklideszi tér (skalárszorzattartó módon) izomorf a standard skalárszorzattal ellátott $\mathbb{R}^n$-nel, ui. $\exists\ \mathcal{E}$ ortonormált bázis, és arra $\langle \mathbf{u},\mathbf{v}\rangle = \langle \sum x_i\mathbf{e}_i, \sum y_j\mathbf{e}_j\rangle = \sum x_iy_i = [\mathbf{u}]_{\mathcal{E}}^T[\mathbf{v}]_{\mathcal{E}}$.

Állítás. Egy V euklideszi tér minden U alterére $V = U \oplus U^\perp$.

Bizonyítás. $U \cap U^\perp = 0$, mert $\langle \mathbf{v},\mathbf{v}\rangle \neq 0$, ha $\mathbf{v} \neq 0$. Így $U + U^\perp = U \oplus U^\perp$. Másrészt tudjuk, hogy $\dim V = \dim U + \dim U^\perp = \dim(U \oplus U^\perp)$, tehát $U \oplus U^\perp = V$. □

Pl.: Komplex vektortéren a standard skalárszorzattal nem működik a Gram–Schmidt-ortogonalizáció, mert pl. $(1,i)(1,i) = 1^2 + i^2 = 1 - 1 = 0$.

Def. komplex euklideszi tér: $V_{\mathbb{C}}$, $\langle\ ,\ \rangle : V \times V \to \mathbb{C}$, amely
hermitikus bilineáris függvény, azaz
$\langle \mathbf{u}+\mathbf{u}',\mathbf{v}\rangle = \langle \mathbf{u},\mathbf{v}\rangle + \langle \mathbf{u}',\mathbf{v}\rangle$
$\langle \mathbf{u},\mathbf{v}+\mathbf{v}'\rangle = \langle \mathbf{u},\mathbf{v}\rangle + \langle \mathbf{u},\mathbf{v}'\rangle$
$\langle \lambda\mathbf{u},\mathbf{v}\rangle = \overline{\lambda}\langle \mathbf{u},\mathbf{v}\rangle$
$\langle \mathbf{u},\lambda\mathbf{v}\rangle = \lambda\langle \mathbf{u},\mathbf{v}\rangle$ (ez a négy feltétel a másféllinearitás), és
$\langle \mathbf{u},\mathbf{v}\rangle = \overline{\langle \mathbf{v},\mathbf{u}\rangle}$ (következésképpen $\langle \mathbf{u},\mathbf{u}\rangle \in \mathbb{R}$)
továbbá pozitív definit:
$\langle \mathbf{u},\mathbf{u}\rangle > 0$, ha $\mathbf{u} \neq \mathbf{0}$.

Jelölés: Valós vagy komplex euklideszi térben $|\mathbf{v}| = \sqrt{\langle \mathbf{v},\mathbf{v}\rangle}$

Pl.: $\mathbb{C}^n$-en $\langle \mathbf{x},\mathbf{y}\rangle = \sum \overline{x}_iy_i$ ilyen. Erre $\langle (1,i),(1,i)\rangle = 1\cdot 1 + (-i)\cdot i = 2$, és általában $\langle \mathbf{x},\mathbf{x}\rangle = \sum \overline{x}_ix_i = \sum |x_i|^2 \geq 0$, és csak akkor 0, ha $x_i = 0\ \forall i$.

Jelölés: $M \in \mathbb{C}^{m\times n}$-re $M^* = \overline{M}^T$, ahol $\overline{M}$-t az M-ből úgy kapjuk, hogy minden elemének a konjugáltját vesszük. Ezzel a jelöléssel a $\mathbb{C}^n$ standard euklideszi skalárszorzata $\langle \mathbf{x},\mathbf{y}\rangle = \mathbf{x}^*\mathbf{y}$. A $*$ művelet műveleti tulajdonságai:

$(A+B)^* = A^* + B^*$
$(AB)^* = B^* A^*$
$A^{**} = A$
$A \in \mathbb{R}^{m\times n}$-re $A^* = A^T$.

Pl.: $A \in \mathbb{C}^{n\times n}$-re $A^* = A$ esetén (azaz, ha A **önadjungált**) $\mathbb{C}^n$-en $\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^* A\mathbf{y}$ hermitikus bilineáris függvény.

Állítás. Minden n-dimenziós komplex euklideszi tér izomorf a standard euklideszi skalárszorzattal ($\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^*\mathbf{y}$) ellátott $\mathbb{C}^n$ térrel.

Bizonyítás. Itt is működik a Gram–Schmidt-ortogonalizáció, és a koordinátázás egy ortonormált bázis szerint skalárszorzattartó izomorfizmus. □

Cauchy–Schwarz–Bunyakovszkij-egyenlőtlenség

Euklideszi térben
$$|\langle \mathbf{u}, \mathbf{v} \rangle| \le |\mathbf{u}| \cdot |\mathbf{v}|.$$
Akkor és csak akkor áll fenn egyenlőség, ha $\mathbf{u} \,||\, \mathbf{v}$.

Háromszög-egyenlőtlenség

Euklideszi térben
$$|\mathbf{u}+\mathbf{v}| \le |\mathbf{u}| + |\mathbf{v}|.$$
Akkor és csak akkor áll fenn egyenlőség, ha $\mathbf{u} \uparrow\uparrow \mathbf{v}$, azaz az egyik vektor a másiknak ≥ 0 valós számszorosa.

Def. Egy valós szimmetrikus / komplex hermitikus bilineáris függvény
pozitív definit, ha $\langle \mathbf{u}, \mathbf{u} \rangle > 0 \ \forall \mathbf{u} \ne \mathbf{0}$
negatív definit, ha $\langle \mathbf{u}, \mathbf{u} \rangle < 0 \ \forall \mathbf{u} \ne \mathbf{0}$
pozitív szemidefinit, ha $\langle \mathbf{u}, \mathbf{u} \rangle \ge 0 \ \forall \mathbf{u}$ (és van $\mathbf{v} \ne \mathbf{0}$: $\langle \mathbf{v}, \mathbf{v} \rangle = 0$)
negatív szemidefinit, ha $\langle \mathbf{u}, \mathbf{u} \rangle \ge 0 \ \forall \mathbf{u}$ (és van $\mathbf{v} \ne \mathbf{0}$: $\langle \mathbf{v}, \mathbf{v} \rangle = 0$)
indefinit, ha $\exists \mathbf{u}, \mathbf{v}$: $\langle \mathbf{u}, \mathbf{u} \rangle > 0$ és $\langle \mathbf{v}, \mathbf{v} \rangle < 0$

Megjegyzés. A pozitív szemidefinit (negatív szemidefinit) általánosabb értelmében magában foglalja a definit esetet is: $\langle \mathbf{u}.\mathbf{u} \rangle \ge 0$ ($\langle \mathbf{u}, \mathbf{u} \rangle \le 0$).

Pl.: Az $A = \begin{bmatrix} 1 & 3 \\ 3 & -1 \end{bmatrix}$ mátrixszal definiált $\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^T A\mathbf{y}$ valós szimmetrikus bilineáris függvény indefinit, mert $\mathbf{e}_1^T A\mathbf{e}_1 = 1 > 0$ és $\mathbf{e}_2^T A\mathbf{e}_2 = -1 < 0$.

Bilineáris függvény mátrixa (Gram-mátrix)

Legyen $\mathcal{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_n\}$ a V egy bázisa, és $\langle\ ,\ \rangle$ valós szimmetrikus vagy komplex hermitikus bilineáris függvény. $\langle\ ,\ \rangle$ **mátrixa** $\mathcal{B}$-ben az A $n \times n$-es mátrix, ha
$$A \text{ elemei } \ a_{ij} = \langle \mathbf{b}_i, \mathbf{b}_j \rangle \quad \forall i, j. \quad \text{Vegyük észre, hogy } A^* = A.$$
Ezt a mátrixot definiálhatjuk azzal is, hogy tetszőleges $\mathbf{u}$, $\mathbf{v}$ vektorokra és $\mathbf{x} = [\mathbf{u}]_{\mathcal{B}}$, $\mathbf{y} = [\mathbf{v}]_{\mathcal{B}}$ koordinátavektoraikra
$$\langle \mathbf{u}, \mathbf{v} \rangle = \mathbf{x}^* A\mathbf{y}.$$
Valóban, $\mathbf{x}^* A\mathbf{y} = \sum_{i,j} \overline{x}_i \langle \mathbf{b}_i, \mathbf{b}_j \rangle y_i = \left\langle \sum_i x_i \mathbf{b}_i, \sum_j y_j \mathbf{b}_j \right\rangle = \langle \mathbf{u}, \mathbf{v} \rangle$.