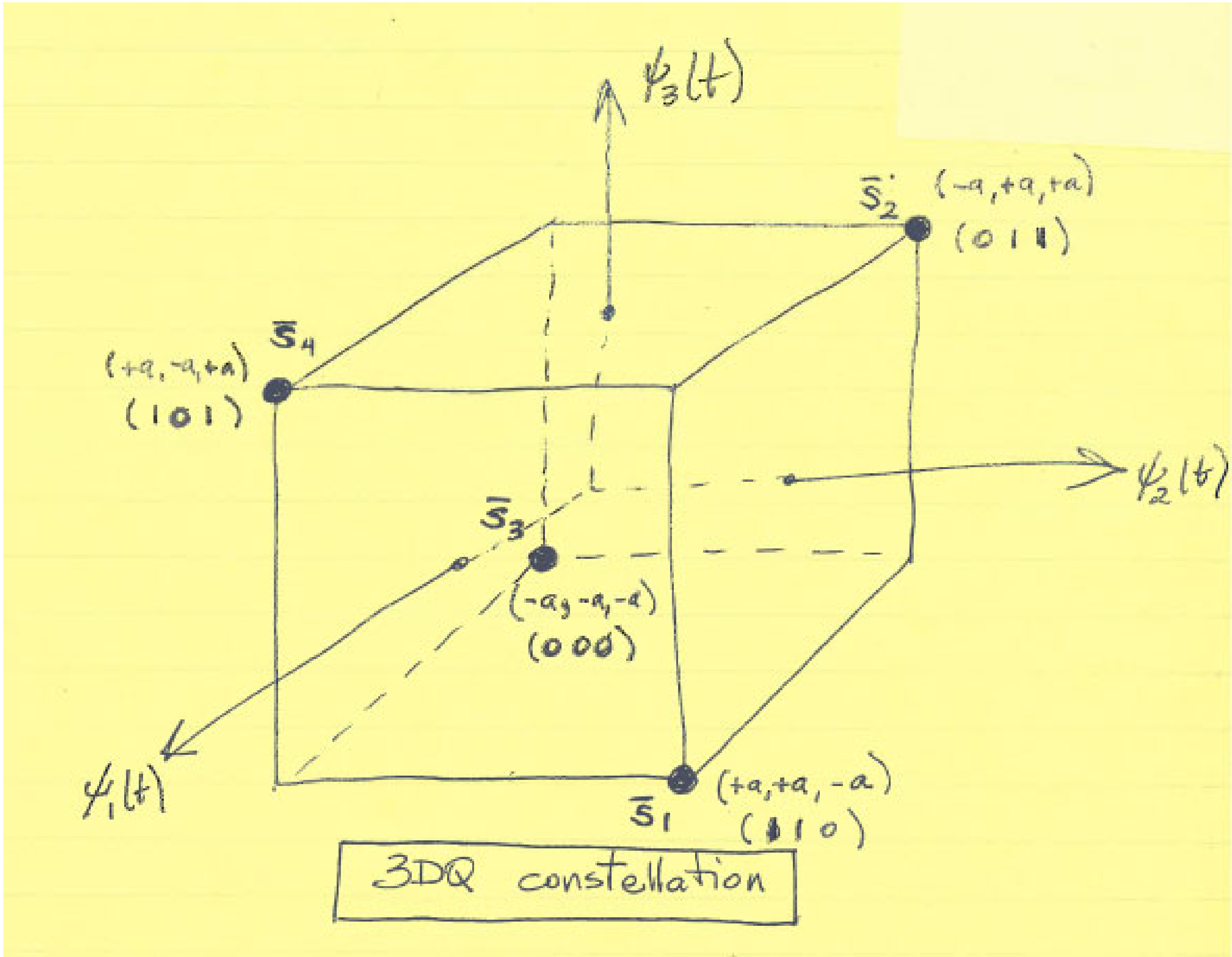
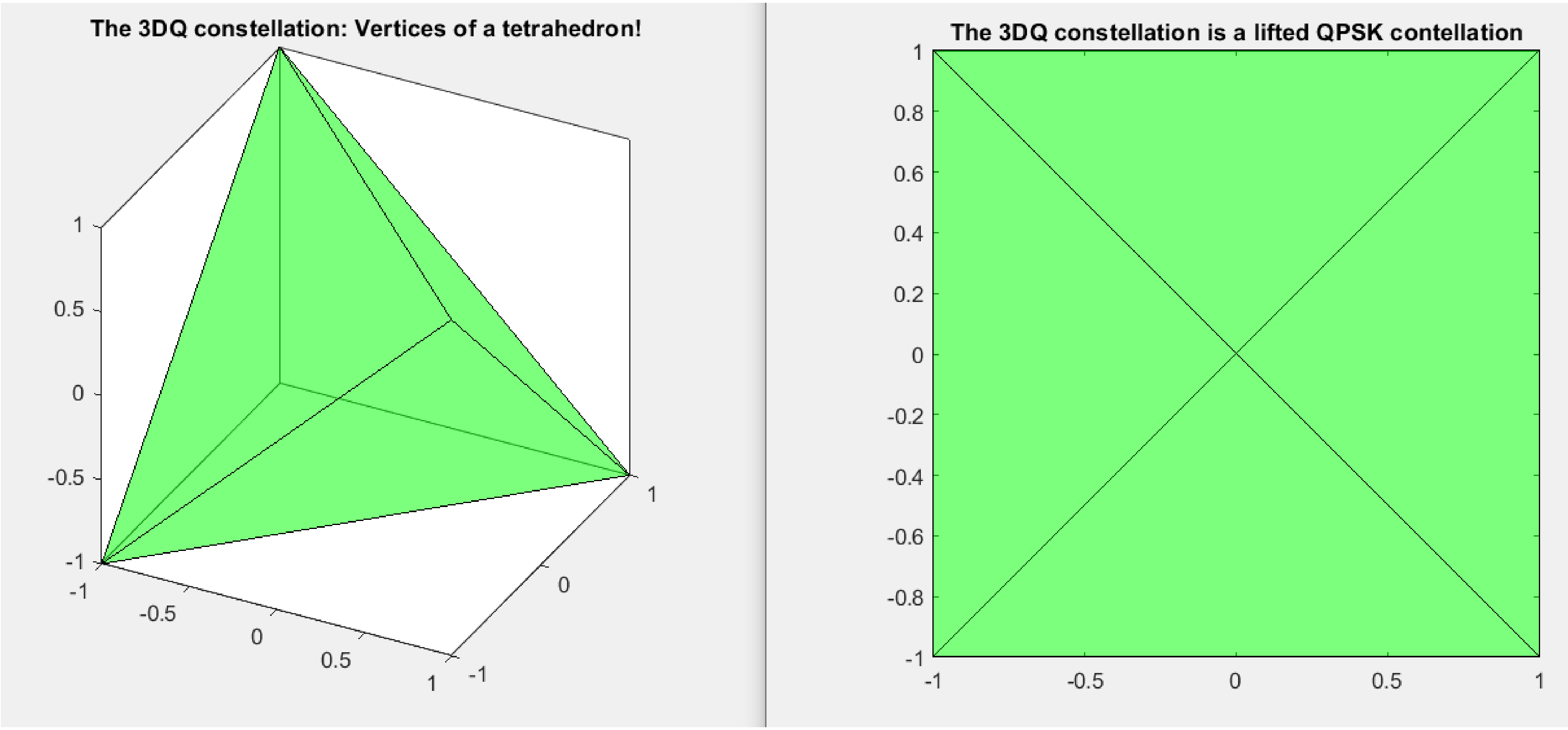


Lecture notes from “11E_MZ_161notes_ECC.pdf”



MATLAB script: “plot_3DQ_constellation.m”

Recall that the syndrome vector, computed from the received vector as $\bar{s} = \bar{r}H^T$ is related to the error vector by the equation

$$\bar{s} = \bar{e}H^T, \tag{1}$$

where *H* is the parity-check matrix. Note that syndrome $\bar{s}$ is an (*n*-*k*)-bit vector.

Eq. (1) above indicates that the syndrome is a function of the error vector, i.e., there is a one-to-one relation between the error vector $\bar{e}$ and the syndrome $\bar{s}$.

The Hamming bound

$$\bar{s} = \bar{e}H^T$$

"To correct up to *t* errors, the number of different syndrome values $\bar{s}$ needs to be greater than or equal to the number of different error vectors $\bar{e}$ with up to *t* ones."

This gives the *Hamming bound*:

$$\boxed{2^{n-k} \geq \sum_{i=0}^{t} \binom{n}{i}}$$

For $t = 1$, or *single-error correcting codes*, the minimum number of different syndrome values is obtained as

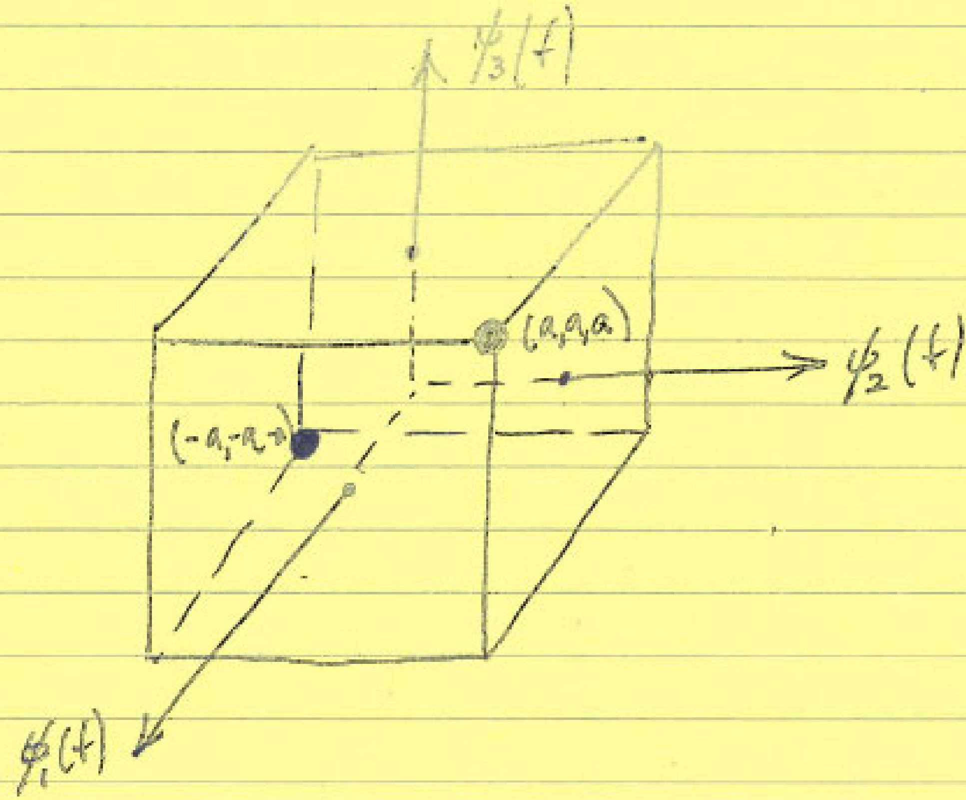
$$2^{n-k} = \sum_{i=0}^{1} \binom{n}{i} = 1 + n \qquad (2)$$

For a single-bit error correcting code, an equivalent statement is that all the columns of H be different. This idea due to Hamming (1949) gives binary linear *Hamming codes*. With $m=n-k$ equal to the number of redundant bits, from Eq. (2) *Hamming codes* have parameters:

Length:	$n = 2^m - 1$
Dimension:	$k = 2^m - 1 - m$
Minimum Hamming distance:	$d_{\min} = 3$

The smallest Hamming code is obtained with *m*=2 and gives the binary linear (3,1,3) repetition code!

Another example: (3,1,3) Binary repetition code



Example: Binary repetition (3,1,3) code

$$G = (1\ 1\ 1), \quad H = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

Error patterns, $\bar{e}$	Syndrome, $\bar{s} = \bar{e}H^T$
$(0\,0\,0)$	$(0\,0)$
$(1\,0\,0)$	$(1\,1)$
$(0\,1\,0)$	$(1\,0)$
$(0\,0\,1)$	$(0\,1)$

Example: If $\bar{c} = (\phi\ \phi\ \phi)$ and $F = (1\ 1\ 0)$

then $\bar{S} = \bar{F} H^T$

$$= (1\ 1\ 0)\begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = (0\ 1)$$

$\longleftrightarrow\ \bar{e} = (0\ 0\ 1)$

From table

$$\therefore\ \hat{c} = \bar{r} \oplus \bar{e} = \begin{array}{r}(1\ 1\ 0)\\ \oplus\ (0\ 0\ 1)\end{array} = (1\ 1\ 1)$$

Hamming (7,4,3) code:

All nonzero column vectors of 3 bits

$$\boxed{H = \left[\begin{array}{cccc:ccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right]} = [P^T \,\vdots\, I_3]$$

Therefore

$$G = [I_4 \,\vdots\, P] = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Suppose information bits $\bar{B} = (0\,1\,1\,0)$. then

$$\bar{C} = (0\,1\,1\,0)\,[G] = \begin{array}{c}(0\,1\,0\,0\,0\,1\,1)\\ + \\ (0\,0\,1\,0\,1\,0\,1)\end{array} = \underline{\underline{(0\,1\,1\,0\,1\,1\,0)}}$$

Suppose error in 4th position, so that

$$\bar{r} = (0\ 1\ 1\ \underset{\uparrow\ \text{error}}{1}\ 1\ 1\ 0)$$

(1) Compute syndrome:

$$\boxed{\bar{S} = \bar{r} H^T} = (0\ 1\ 1\ 1\ 1\ 1\ 0) \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = (1\ 1\ 1).$$

Homework:
Write as equations/circuit

(2) This corresponds to the 4th column of H.
transpose of the

∴ Error in 4th position

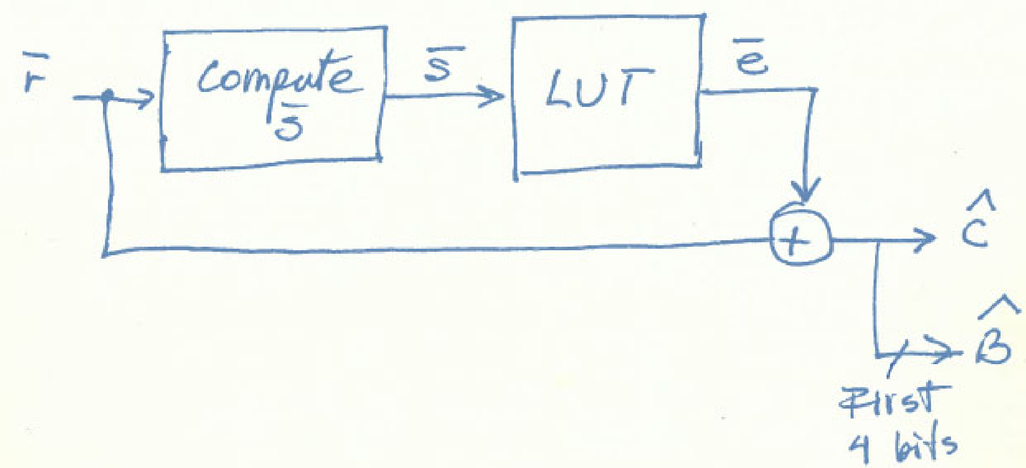
$$\hat{C} = (\underbrace{0\ 1\ 1\ 0}_{\text{Information bits}}\ 1\ 1\ 0) \rightarrow (0\ 1\ 1\ 0) = \hat{B}$$

Look-up table :

Syndrome $\bar{s}$	Error vector $\bar{e}$
0 0 0	0 0 0 0 0 0 0
1 1 0	1 0 0 0 0 0 0
0 1 1	0 1 0 0 0 0 0
1 0 1	0 0 1 0 0 0 0
1 1 1	0 0 0 1 0 0 0
1 0 0	0 0 0 0 1 0 0
0 1 0	0 0 0 0 0 1 0
0 0 1	0 0 0 0 0 0 1

H^T

HD decoder :



SJSU SAN JOSÉ STATE UNIVERSITY

The log-likelihood (log of the conditional prob.) (*)

$$\log\left(p(\bar{Y}|\bar{s})\right) = L(\bar{c})$$

can be written as

$$L(\bar{c}) = \sum_{i=1}^{n} s_i Y_i$$

$$\boxed{L(\bar{c}) = \sum_{i=1}^{n} m(c_i) Y_i},$$ correlation

where Y_i denote MF outputs

Soft-decision decoding

Choose as the most likely transmitted codeword $\bar{c} = \bar{B}G$, the one that maximizes $L(\bar{c})$

(*) $$p(\bar{Y}|\bar{s}) = \frac{1}{(\sqrt{\pi N_0})^n} \cdot e^{-\frac{1}{N_0}\sum_{i=1}^{n}(Y_i - s_i)^2}$$

$s_i = \pm\sqrt{E}$ for BPSK (polar)

SJSU SAN JOSÉ STATE UNIVERSITY

EE161

CORRELATIONS OF (3,2,2) EPC CODE

Map: $0 \to +1$, $1 \to -1$

Uncoded $B_1\ B_2$	Coded $C_1\ C_2\ C_3$	$\bar{S}$	Correlations ρ
0 0	0 0 0	a a a	$Y_1 + Y_2 + Y_3$
0 1	0 1 1	a -a -a	$Y_1 - Y_2 - Y_3$
1 1	1 1 0	-a -a a	$-Y_1 - Y_2 + Y_3$
1 0	1 0 1	-a a -a	$-Y_1 + Y_2 - Y_3$

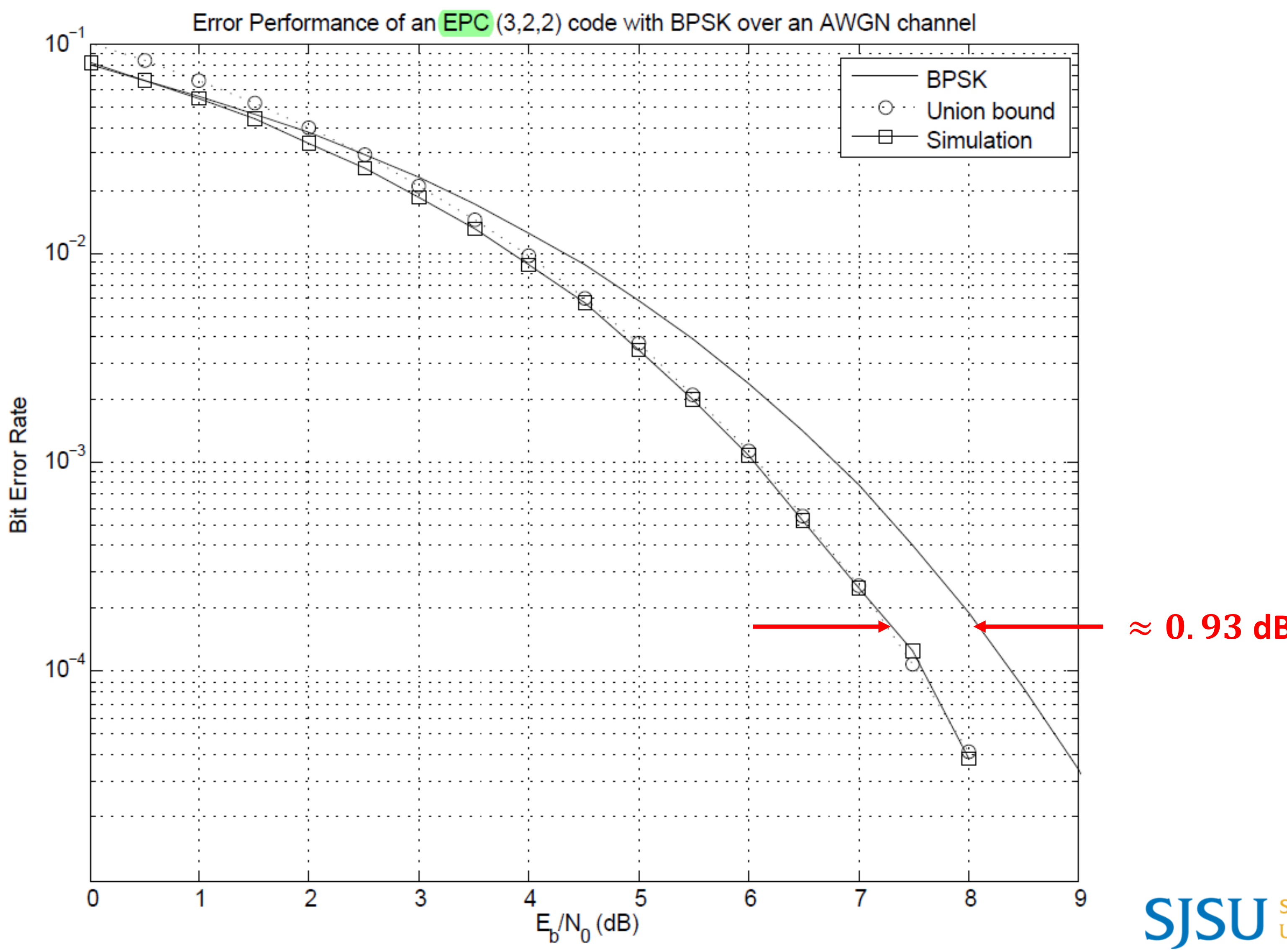
$a = \sqrt{E_s/3}$

MAP: $0 \to -a$

$1 \to +a$

$B_1\ B_2$	$C_1\ C_2\ C_3$	$\bar{S}$	Correlations ρ
0 0	0 0 0	-a -a -a	$-Y_1 - Y_2 - Y_3$
0 1	0 1 1	-a +a +a	$-Y_1 + Y_2 + Y_3$
1 1	1 1 0	+a +a -a	$+Y_1 + Y_2 - Y_3$
1 0	1 0 1	+a -a +a	$+Y_1 - Y_2 + Y_3$

SJSU SAN JOSÉ STATE UNIVERSITY



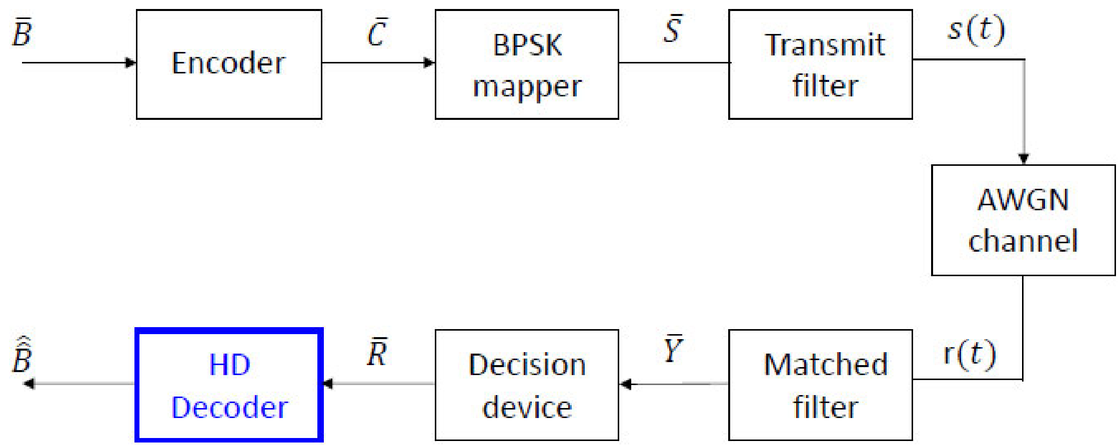
SJSU SAN JOSÉ STATE UNIVERSITY

Hard-decision (HD) decoding versus soft-decision (SD) decoding

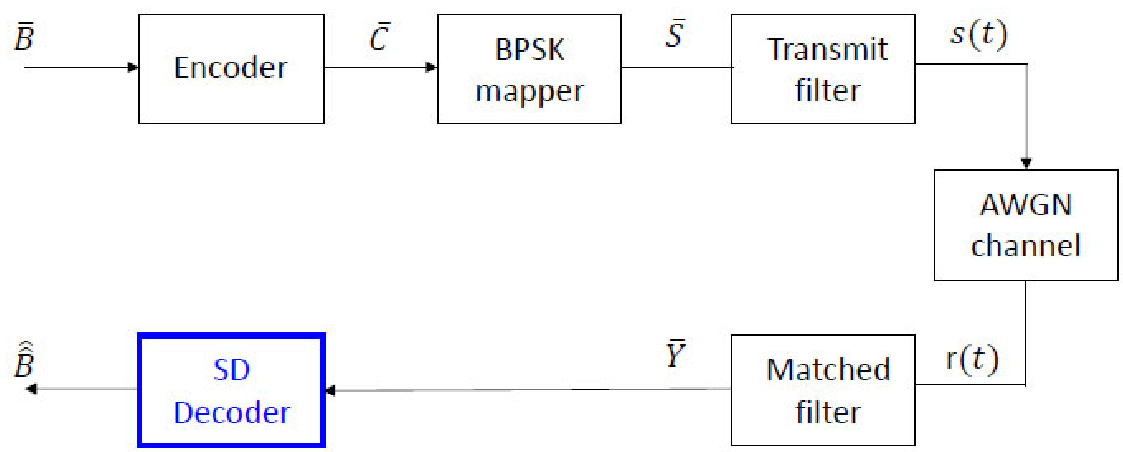
- HD decoding: Correct errors after ML estimation (decision device), R_k
- SD decoding: Use of matched-filter outputs, Y_k

SD decoding performs better than HD decoding, as the *combined likelihood of all coded bits* is used instead of bit-by-bit decisions

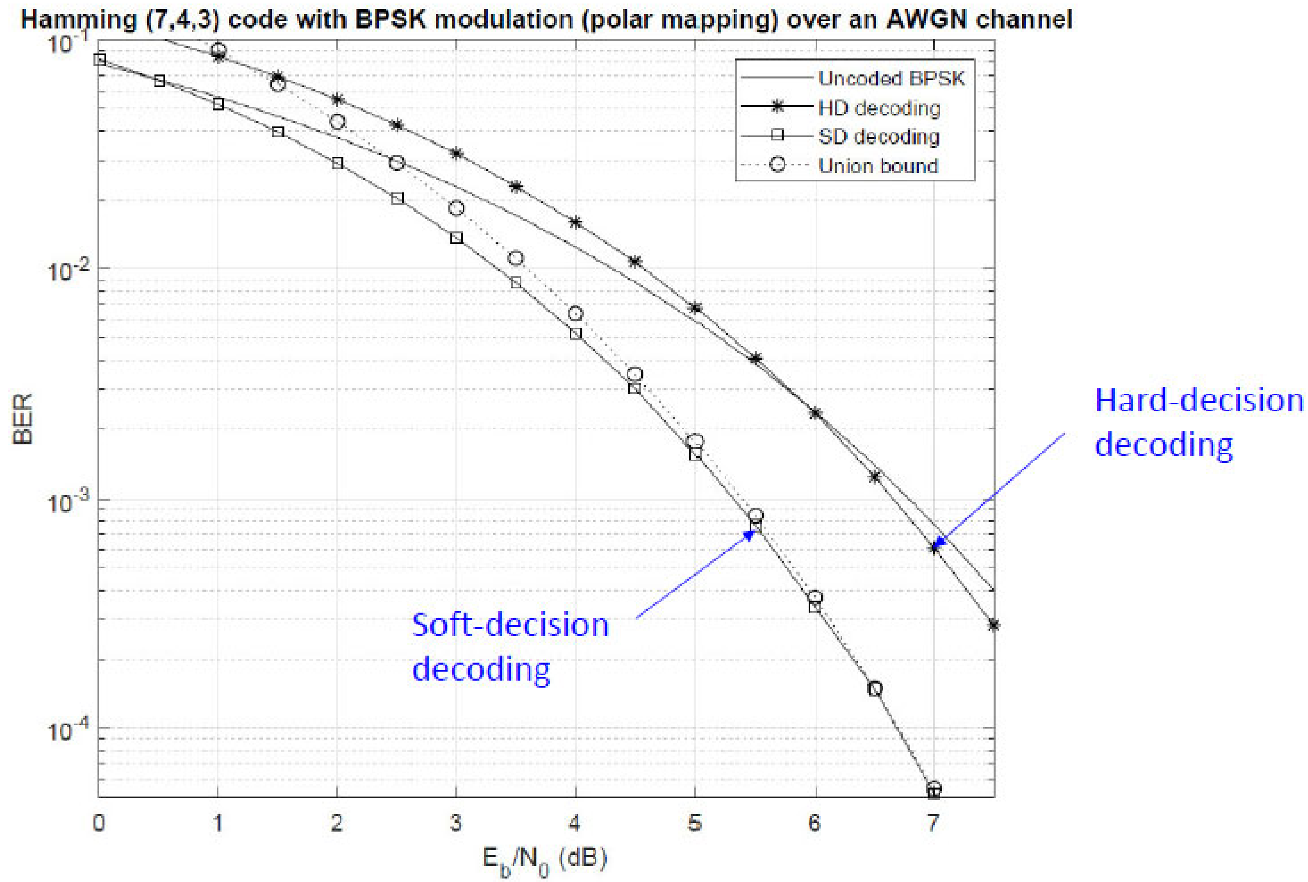
Hard-decision decoding



Soft-decision decoding



Example: Binary Hamming (7,4,3) code



Coding gain and "real" (effective) coding gain

$\boxed{\text{Binary } (n, k, d_{min}) \text{ codes with polar mapping over AWGN}}$

Modulated codeword : $\bar{S} = (\pm a, \pm a, \ldots, \pm a)$

$$= a \cdot \left((-1)^{B_1}, (-1)^{B_2}, \ldots, (-1)^{B_n}\right)$$

Average symbol energy : $n \cdot a^2 = E_s \Rightarrow a = \sqrt{E_s/n}$

Each codeword carries k bits, therefore $E_s = k E_b$

or

$$a = \sqrt{\frac{k}{n} E_b}$$

note, this is the fake energy

The min. Euclidean distance between modulated codewords is $d^E_{min} = \sqrt{4 d_{min} \cdot a^2}$

$\sqrt{d_{min} (2a)^2}$

SJSU SAN JOSÉ STATE UNIVERSITY

Finally, the pairwise error probability between modulated codewords is

$$\boxed{P_2 = Q\left(\sqrt{d_{min}\frac{k}{n}\frac{2E_b}{N_0}}\right)} \qquad \left(= Q\left(\sqrt{\frac{d^2}{2N_0}}\right).\right)$$

At high values of E_b/N_0, the average probability of a bit error

$$\boxed{P_b \approx Q\left(\sqrt{\underbrace{d_{min}\cdot\frac{k}{n}}_{\text{ASYMPTOTIC CODING GAIN} = CG}\cdot\frac{2E_b}{N_0}}\right)} = Q\left(\sqrt{R\cdot d_{min}\frac{2E_s}{N_0}}\right)$$

Code	d_{min}	k/n	CG (dB)
(3,2,2)	2	2/3	1.25
(4,3,2)	2	3/4	1.76
(7,4,3)	3	4/7	2.34

This asymptotic coding gain does not take into account the number of codewords at minimum distance, $A_{d_{min}}$.

The loss due to this number is approx. $0.2 \log_2 (A_{d_{min}})$ so that the coding gain can be better as

Real Coding Gain

$$RCG \approx 10 \log_{10}\left(d_{min} \cdot \frac{k}{n}\right) - 0.2 \log_2 (A_{d_{min}}) \quad (dB)$$

Code	RCG	$A_{d_{min}}$
(3,2,2)	0.93	3
(4,3,2)	1.24	6
(7,4,3)	1.78	7