Reliability-based SD decoding

a) Not applicable to only graph-based codes
   - May even help with some algebraic structure
b) SD alternative to trellis decoding and iterative decoding
   - It is hard to implement ML SD decoding for general codes
c) Performance: Somewhere between HD decoding and ML SD decoding

Correlation discrepancy

a) Send binary codeword $\mathbf{v} = (v_0, \ldots, v_{n-1})$

b) Modulate into bipolar $\mathbf{c} = (c_0, \ldots, c_{n-1})$ ($0 \longrightarrow -1$ and $1 \longrightarrow 1$)

c) Received real vector $\mathbf{r} = (r_0, \ldots, r_{n-1})$

d) $P(r_i|v_i) = K \cdot \mathrm{e}^{-(r_i - c_i)^2/N_0}$ (AWGN channel)

e) $P(r_i|v_i = 1)/P(r_i|v_i = 0) = K \cdot \mathrm{e}^{-(r_i-1)^2/N_0} / K \cdot \mathrm{e}^{-(r_i+1)^2/N_0}$

f) $\log(P(r_i|v_i = 1)/P(r_i|v_i = 0)) \propto r_i$

g) Decode to the modulated codeword c that minimizes

$$\sum_i (r_i - c_i)^2 = \sum_i r_i^2 + n - 2 \sum_i r_i \cdot c_i$$

h) Maximize correlation $m(\mathbf{r},\mathbf{v}) = \sum_i r_i \cdot c_i$

i) $= \sum_i |r_i| - 2 \sum_{i \text{ such that } r_i \cdot c_i < 0} |r_i|$

j) Minimize correlation discrepancy $\lambda(\mathbf{r},\mathbf{v}) = \sum_{i \text{ such that } r_i \cdot c_i < 0} |r_i|$ 2

Reliability measures and decoding

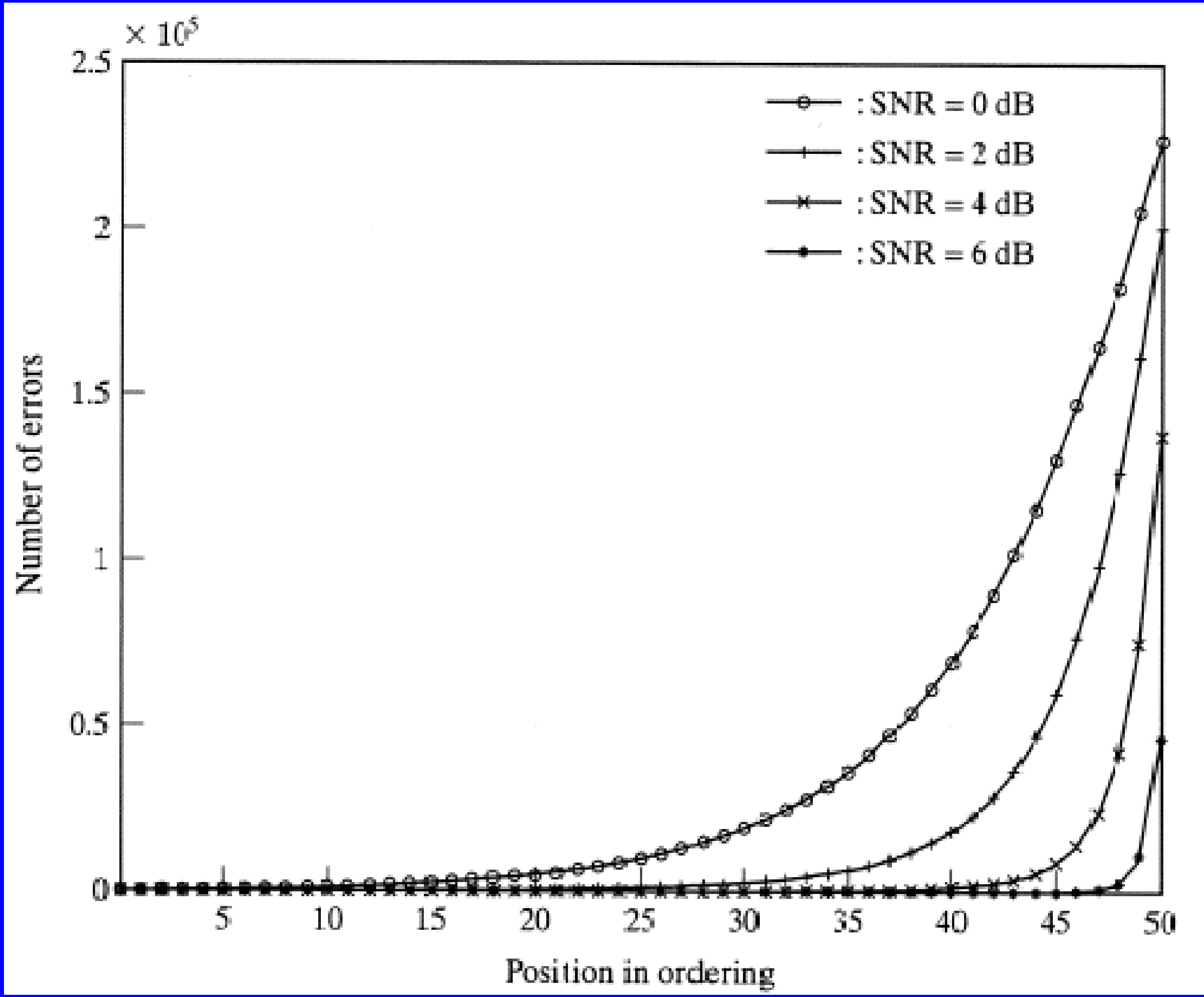
a) Consider the received vector $\mathbf{r}$

b) For each received symbol r_i form the hard decision $z_i=0$ for $r_i < 0$ and $z_i=1$ otherwise

c) The reliability $|\log(P(r_i|v_i=1)/P(r_i|v_i=0))| \propto |r_i|$

d) As can be expected, z_i is more likely to be in error when $|r_i|$ is small

Probability of error in z_i: LRP vs MRP



Reliability and decoding: LRP

a) Decoding based on the set of least reliable positions (LRPs)

b) Assume that errors are more likely to occur in the LRPs

- Select a set E of error patterns $\mathbf{e}$, confined to the LRPs
- For each $\mathbf{e} \in E$, form the modified vector $\mathbf{z}+\mathbf{e}$
- Decode $\mathbf{z}+\mathbf{e}$ into a codeword $\mathbf{c}(\mathbf{e}) \in C$ by use of an efficient algebraic decoder
- The preceding steps give a list of candidate codewords. The final decoding step is to compare each of these codewords with $\mathbf{r}$, and select the one which is closest in terms of squared Euclidean distance or correlation discrepancy

c) *Performance: Depends on* $|E|$

d) *Complexity: Depends on* $|E|$ *and on the algebraic decoder*

Reliability and decoding: MRP

a) Decoding based on the set of most reliable positions (MRPs)

b) Assume that errors are less likely to occur in the MRPs
   - Select a set I of k independent MRPs (MRIPs). A set of k independent positions in $\mathbf{z}$ determines a codeword
   - Select a set E of low-weight error patterns $\mathbf{e}$ of length k
   - For each $\mathbf{e} \in E$, form the modified information vector $\mathbf{z}_k+\mathbf{e}$ and encode it into a codeword $\mathbf{c}(\mathbf{e}) \in C$ where $\mathbf{z}_k$ consists of the symbols of $\mathbf{z}$ at the k MRIPs
   - The preceding steps give a list of candidate codewords. The final decoding step is to compare each of these codewords with $\mathbf{r}$, and select the one which is closest in terms of squared Euclidean distance or correlation discrepancy

c) *Performance and complexity: Depends on* $|E|$

Condition on optimality

a) In both of the preceding algorithms, whenever we find a codeword which is *good enough*, we can terminate the process

b) What do we mean by *good enough*?

c) We need an optimality condition

Condition on optimality (cont.)

- $D_0(\mathbf{v}) = \{i : v_i = z_i,\ 0 \le i < n\}$, $D_1(\mathbf{v}) = \{i : v_i \ne z_i,\ 0 \le i < n\}$
- $n(\mathbf{v}) = |\ D_1(\mathbf{v})\ | = d_H(\mathbf{v},\mathbf{z})$
- $\lambda(\mathbf{r},\mathbf{v}) = \sum_{i \text{ such that } r_i \cdot c_i < 0} |r_i| = \sum_{i \in D_1(\mathbf{v})} |r_i|$
- Want to find the codeword with the lowest correlation discrepancy
- If there exists a codeword $\mathbf{v}^*$ such that $\lambda(\mathbf{r},\mathbf{v}^*) \le \alpha(\mathbf{r},\mathbf{v}^*) = \min_{\mathbf{v} \in C,\ \mathbf{v} \ne \mathbf{v}^*} \{\lambda(\mathbf{r},\mathbf{v})\}$, then $\mathbf{v}^*$ is the ML codeword
- $\alpha(\mathbf{r},\mathbf{v}^*)$ is hard to evaluate, but we can hope to find a lower bound on it, which gives a sufficient condition for $\mathbf{v}^*$ to be the ML codeword
- Let $D_0^{(j)}(\mathbf{v})$ consist of the j elements of $D_0(\mathbf{v})$ with lowest reliability $|r_i|$. For $j \le 0$, $D_0^{(j)}(\mathbf{v}) = \{\}$ and for $j \ge |D_0(\mathbf{v})|$, $D_0^{(j)}(\mathbf{v}) = D_0(\mathbf{v})$
- Let w_i be the ith nonzero weight in the code

Condition on optimality (cont.)

a) Thus, $D_0^{(w_j-n(\mathbf{v}))}(\mathbf{v})$ consists of the w_j-$n(\mathbf{v})$ elements of $D_0(\mathbf{v})$ with lowest reliability $|r_i|$

b) **Theorem**: If

$$\lambda(\mathbf{r},\mathbf{v}) \le \sum_{i\in D_0^{(w_j-n(\mathbf{v}))}(\mathbf{v})} |r_i|,$$

then the ML codeword for **r** is at a distance less than w_j from **v**

c) **Proof**: Assume that **v'** is a codeword such that $d_H(\mathbf{v},\mathbf{v'}) \ge w_j$

- $\lambda(\mathbf{r},\mathbf{v'}) = \sum_{i\in D_1(\mathbf{v'})} |r_i| \ge \sum_{i\in D_0(\mathbf{v}) \cap D_1(\mathbf{v'})} |r_i|$
  $\ge \sum_{i\in D_0^{(w_j-n(\mathbf{v}))}(\mathbf{v})} |r_i|,$
- ...because $|D_1(\mathbf{v'})| \ge |D_0(\mathbf{v}) \cap D_1(\mathbf{v'})| \ge w_j - n(\mathbf{v})$:
  - $|D_0(\mathbf{v}) \cap D_1(\mathbf{v'})| + |D_1(\mathbf{v}) \cap D_0(\mathbf{v'})| = d_H(\mathbf{v},\mathbf{v'}) \ge w_j$
  - $|D_1(\mathbf{v'})| \ge |D_0(\mathbf{v}) \cap D_1(\mathbf{v'})| \ge w_j - |D_1(\mathbf{v}) \cap D_0(\mathbf{v'})|$
    $\ge w_j - |D_1(\mathbf{v})| \ge w_j - n(\mathbf{v})$

Corollary

a) If

$$\lambda(\mathbf{r},\mathbf{v}) \leq \sum_{i \in D_0{}^{(w_1 - n(\mathbf{v}))}(\mathbf{v})} |r_i|,$$

then **v** is the ML codeword

b) If

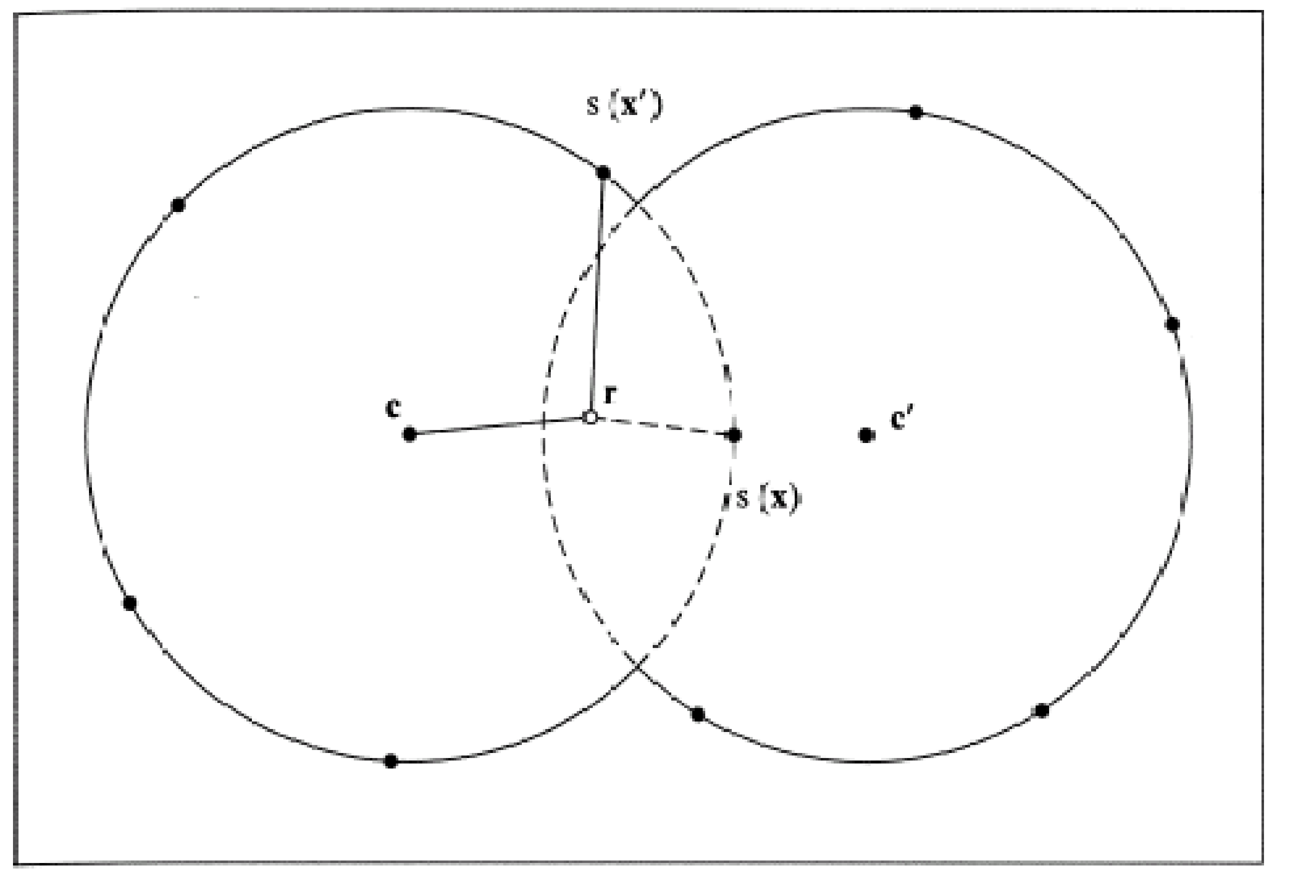
$$\lambda(\mathbf{r},\mathbf{v}) \leq \sum_{i \in D_0{}^{(w_2 - n(\mathbf{v}))}(\mathbf{v})} |r_i|,$$

then either **v** is the ML codeword, or the ML codeword is one of the nearest neighbours of **v**

Optimality condition based on two observed codewords

a) A more sophisticated criterion can be applied if we know more than one codeword "close" to **r**

b) Skip the details



Generalized minimum distance decoding

a) Forney (1966)
b) Based on error and erasure decoding
c) Consider two codewords **c** and **c'** such that $d = d_H(\mathbf{c},\mathbf{c}')$. Assume that **c** is sent
d) Assume an error and erasure channel producing t errors and e erasures
e) Then, an ML decoder will decode to **c** if

$$2t+e \leq d - 1$$

f) GMD decoding considers patterns of $\leq d_{\min} - 1$ erasures in the $d_{\min} - 1$ LRPs

GMD decoding (on an AWGN)

a) From **r**, derive the HD word **z** and the reliability word |**r**|

b) Produce a list of $\lfloor (d_{\min}+1)/2 \rfloor$ partly erased words by erasing

- If $d_{\min}$ is even; the least reliable, the three least reliable, ..., the $d_{\min}$ - 1 least reliable positions
- If $d_{\min}$ is odd; no bit, the two least reliable, the four least reliable, ..., the $d_{\min}$ - 1 least reliable positions

c) For each partly erased word in the list, decode by using (algebraic) error and erasure decoding algorithm

d) Compute SD decoding metric for each decoded word w.r.t **r**. Select the one closest to **r**

e) A sufficient condition on optimality can be used for early stopping

The Chase algorithms: 1

a) From **r**, derive the HD word **z** and the reliability word |**r**|
b) Produce a set E of all error patterns of weight exactly $\lfloor d_{\min}/2 \rfloor$
c) For each $\mathbf{e} \in E$, decode **z+e** by using (algebraic) errors-only decoding algorithm
d) Compute SD decoding metric for each decoded word w.r.t **r**. Select the one closest to **r**
e) A sufficient condition on optimality can be used for early stopping
f) Better performance, but veeeery high complexity

The Chase algorithms: 2

a) From **r**, derive the HD word **z** and the reliability word |**r**|
b) Produce a set of $2^{\lfloor d_{\min}/2 \rfloor}$ test error patterns E with all possible error patterns confined to the $\lfloor d_{\min}/2 \rfloor$ LRPs
c) For each $\mathbf{e} \in E$, decode **z+e** by using (algebraic) errors-only decoding algorithm
d) Compute SD decoding metric for each decoded word w.r.t **r**. Select the one closest to **r**
e) A sufficient condition on optimality can be used for early stopping
f) Better performance, but higher complexity than Chase-3 to be described next

The Chase algorithms: 3

a) From **r**, derive the HD word **z** and the reliability word |**r**|

b) Produce a list of $\lfloor d_{min}/2+1 \rfloor$ modified words by complementing

- If d_{min} is even; no bit, the least reliable, the three least reliable, ..., the d_{min} -1 least reliable positions
- If d_{min} is odd; no bit, the two least reliable, the four least reliable, ..., the d_{min} -1 least reliable positions

c) For each modified word in the list, decode by using (algebraic) errors-only decoding algorithm

d) Compute SD decoding metric for each decoded word w.r.t **r**. Select the one closest to **r**

e) A sufficient condition on optimality can be used for early stopping

Generalized Chase and GMD decoding

a) Generalizations: How to choose the test error patterns

b) Choose a number $a \in \{1,2,\ldots,\lceil d_{\min}/2 \rceil\}$

c) Algorithm $A(a)$ uses error set $E(a)$ consisting of the following $2^{a-1}(\lceil (d_{\min}+1)/2 \rceil - a+1)$ vectors

- For even $d_{\min}$:
  - All 2^{a-1} error patterns confined to the a-1 LRPs
  - For each of the preceding error patterns, also complement the i next LRPs, i=0,1,3,..., $d_{\min}-2a+1$
- For odd $d_{\min}$:
  - All 2^{a-1} error patterns confined to the a-1 LRPs
  - For each of the preceding error patterns, also complement the i next LRPs, i=0,2,4,..., $d_{\min}-2a+1$

The generalized Chase algorithm $A(a)$

a) From **r**, derive the HD word **z** and the reliability word |**r**|
b) Generate the error patterns in $E(a)$ (in likelihood order?)
c) For each modified word in the list, decode by using (algebraic) errors-only decoding algorithm
d) Compute SD decoding metric for each decoded word w.r.t **r**. Select the one closest to **r**
e) A sufficient condition on optimality can be used for early stopping
f) Note that $A(1)$ is Chase-3
g) Note that $A(\lceil d_{\min}/2 \rceil)$ is Chase-2
h) Note that $A(a)$ achieves bounded distance decoding, i.e., if the received sequence is within a distance of sqrt($d_{\min}$) of the sent word, then decoding is correct

The generalized GMD algorithm $A_e(a)$

a) Similar to $A(a)$, but uses error set $E_e(a)$ formed by (even $d_{\min}$):
   - All 2^{a-1} error patterns confined to the a-1 LRPs
   - For each of the preceding error patterns, also erase the i next LRPs, i=1,3,..., $d_{\min}$-2a+1

b) Decode with algebraic error and erasure decoder

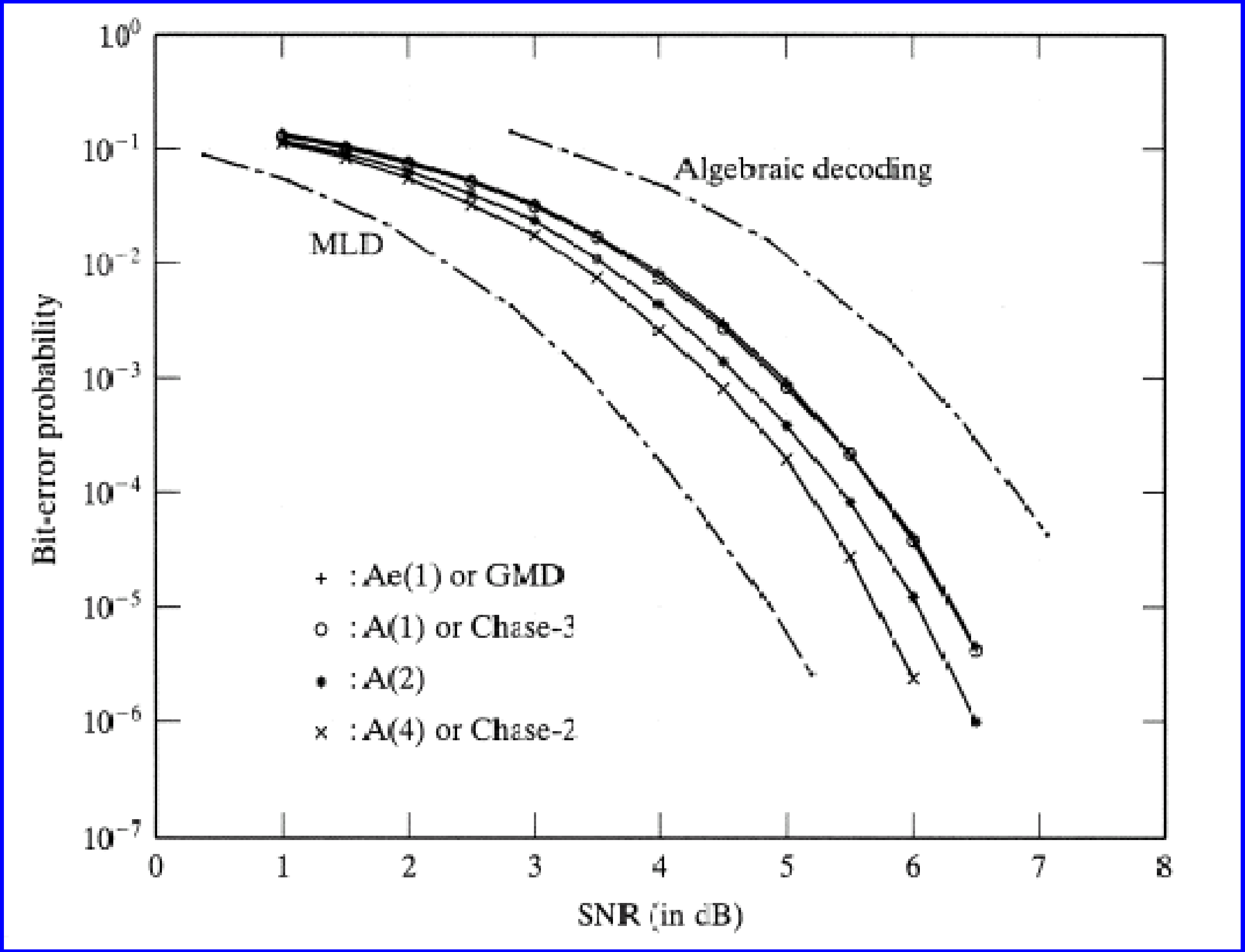
c) Generates $\leq 2^{a-1}(\lceil d_{\min}/2 \rceil - a + 1)$ candidate codewords

d) Note that $A_e(1)$ is the basic GMD decoder

e) Note that $A_e(a)$ achieves bounded distance decoding, i.e., if the received sequence is within a distance of sqrt($d_{\min}$) of the sent word, then decoding is correct

f) Similar to $A(a)$ in basic properties (performance, complexity)

Performance curves: (64,42,8) RM code



Performance curves: (127,64,21) BCH code