

II. Bounds on Error Correction Capabilities

References:

Peterson - Ch 4, Berlekamp - Ch 13

Interested in bounds on R and N for given error correction capability.

Can use bounds later on to see how good the codes we come up with are.

A. Elspas Bound

a linear code that corrects all patterns of t or fewer errors must contain at least $2t$ check digits (i.e. $N-K \geq 2t$)

Proof: $d_{\min} \geq 2t+1$ so no $2t$ or less columns of H are linearly dependent. H can be reduced to echelon canonical form and since it has rank $N-K$, reduction will have $N-K$ ^{distinct} columns with one 1 and $N-K-1$ zeros. These columns can be combined to form any vector of length $N-K$. Therefore there will ~~be~~ always be a set of $N-K+1$ columns of H that are linearly dependent.

Thus $N-K+1 \geq d_{\min} \geq 2t+1$

Q.E.D.

Remark: For binary repetition code with

$$N \text{ odd } t = \frac{N-1}{2}, K=1 \text{ so } N-K = 2t$$

Can show this is only binary linear code that meets bound. (Non binary codes exist)

that meet bound) (Reed-Solomon codes)

If bound met with equality, code called a maximum distance separable code.

B. Hamming Bound

Let $V_r(\bar{x}) =$ number of N -tuples with Hamming distance $\leq r$ from $\bar{x}$. Then

$$V_r(\bar{x}) = \sum_{i=0}^{r+1} \binom{N}{i} (q-1)^i$$

Notice that this is independent of $\bar{x}$. A distance measure called isocentric if this is true.

An (N, K) linear code which corrects all patterns of t or fewer errors requires at least $\log_q V_t$ check digits. That is,

$$N-K \geq \log_q \sum_{i=0}^t \binom{N}{i} (q-1)^i$$

Proof: Need distinct syndrome for each correctable error pattern. So need at least

$$\sum_{i=0}^t \binom{N}{i} (q-1)^i = V_t$$

syndromes. For (N, K) code there are

q^{N-K} syndromes. Thus $V_t \leq q^{N-K}$

Q.E.D.

Remark: If bound met code called perfect.

EX. Binary Repetition code with N odd, Hamming

single error correcting binary code, Golay

(23, 12), Golay (11, 6) $t=2$ code over $GF(3)$

Notice that $\sum_{i=0}^2 \binom{q^0}{i} = 2^{1/2}$, however, code not known for this case.

Hamming bound holds also for non-linear block codes.

Proof: (sphere packing argument)

Pick $M = q^{NR} = q^K$ code words. If code corrects t errors or less there must be

V_t received words decoded to each code word. There are q^N possible received words, so that

$$M V_t \leq q^N \Rightarrow V_t \leq q^{N-K}$$

G.E.D.

Asymptotic Bound for Binary Case ($q=2$)

Lemma: (J.M. Vozenkraft + B. Reiffen,

Sequential Decoding, MIT Press, 1961, appendix)

For $0 < \lambda < 1$, $n\lambda$ an integer

$$\frac{1}{\sqrt{8n\lambda(1-\lambda)}} 2^{nH(\lambda)} \leq \binom{n}{n\lambda} \leq \frac{1}{\sqrt{2\pi n\lambda(1-\lambda)}} 2^{nH(\lambda)}$$

where $H(\lambda) = -\lambda \log \lambda - (1-\lambda) \log (1-\lambda)$

So for large N , from Hamming bound

$$2^{N-K} \geq \sum_{i=0}^t \binom{N}{i} \geq \binom{N}{t} \geq \frac{1}{\sqrt{8N\lambda(1-\lambda)}} 2^{NH(\lambda)}$$

with $N\tau = t$. Take $\log_2$ of both sides

$$N - K \geq -\frac{1}{2} \log_2 8t(1 - \frac{t}{N}) + NH(\tau)$$

$$\text{or } H(\tau) \leq 1 - R + \frac{1}{2N} \log_2 8t(1 - \frac{t}{N})$$

$$\text{let } O_1(N) = \frac{1}{2N} \log_2 8t(1 - \tau)$$

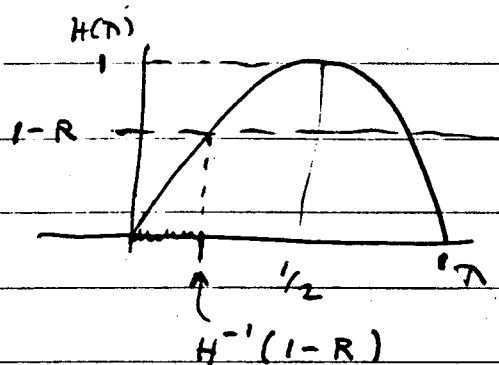
$$\text{so } \lim_{N \rightarrow \infty} O_1(N) = 0 \quad \text{for } \tau = \frac{t}{N} \text{ fixed}$$

i.e. as increase block length N , keep percentage of correctable errors t/N constant. Then

$$H(\tau) \leq 1 - R + O_1(N)$$

For large N , $t \leq d_{\min}/2$ and $d_{\min} \leq N$

$$\text{so } 0 \leq \tau \leq 1/2$$



Theorem: (asymptotic Hamming Bound)

$$\lim_{N \rightarrow \infty} \frac{t}{N} = \frac{d_{\min}}{2N} \leq H^{-1}(1 - R)$$

Plotted on p. 50 of Peterson

$$R < 1 - H\left(\frac{d_{\min}}{2N}\right)$$

C. Varshamov, Gilbert, Sacks Bound
(p. 51 Peterson)

An (N, K) code exists with minimum distance $d_{\min}$, with $N-K$ as the smallest integer satisfying

$$\sum_{i=0}^{d_{\min}-2} \binom{N-1}{i} (q-1)^i < q^{N-K}$$

Proof: Construct H so that no set of $d_{\min}-1$ or fewer columns are linearly dependent. Select any nonzero $N-K$ tuple as first column of H . Select any nonzero $N-K$ tuple except multiples of the first as second column. Third column chosen to be linearly independent of first two. In general i^{th} column chosen linearly independent of any $d_{\min}-2$ or fewer previous columns. This insures no linear combination of $d_{\min}-1$ or fewer columns linearly dependent.

As long as set of all linear combinations of $d_{\min}-2$ or fewer columns does not include all $N-K$ tuples, another column can be added. In worst case ^{in sense of using up most number of possible columns} all these linear combinations distinct. Assume all distinct.

Then from $N-1$ columns there are $\binom{N-1}{i}$ ways of choosing i columns. There are $(q-1)^i$ ways of combining i columns. Thus there are

$$\sum_{i=1}^{d_{\min}-2} \binom{N-1}{i} (q-1)^i$$

linear combinations of $d_{\min}-2$ or less columns out of $N-1$ columns. There are $q^{N-K}-1$ possible nonzero columns. So if

$$\sum_{i=1}^{d_{\min}-2} \binom{N-1}{i} (q-1)^i < q^{N-K}-1$$

another column can be chosen.

Q.E.D.

D. Gilbert Bound

Slightly weaker than V-G-S bound but holds for any block code, linear or nonlinear.

A block code of length N exists with minimum distance $d_{\min}$ having ~~no more than $N-K$ check~~ $M = q^K$ code words if

$$q^{N-K} \geq \sum_{i=0}^{d_{\min}-1} \binom{N}{i} (q-1)^i$$

Proof: construct code by following algorithm

- (0) Begin with $\mathcal{L}$ as set of all N tuples and set i to 1.

(1) Choose as codeword $\vec{x}_i$ any N -tuple in $\mathcal{L}$

(2) Delete from $\mathcal{L}$ any $\vec{y}$ such that $d(\vec{x}_i, \vec{y}) < d_{\min}$

(3) If $\mathcal{L}$ empty, stop. Otherwise increase i by one and return to (1)

Clearly all codewords separated by distance at least $d_{\min}$. At each step can delete at most $V_{d_{\min}-1} = \sum_{i=0}^{d_{\min}-1} \binom{N}{i} (q-1)^i$

N -tuples from $\mathcal{L}$. Hence algorithm doesn't terminate if

$$M V_{d_{\min}-1} \leq q^N$$

$$\text{or } V_{d_{\min}-1} \leq q^{N-K}$$

Q.E.D.

Asymptotic Bound for $q=2$

Lemma (Wozencraft + Reiffen, appendix)

For $0 < \epsilon < 1$

$$\sum_{i=0}^{\lfloor N\epsilon \rfloor} \binom{N}{i} \epsilon^i (1-\epsilon)^{N-i} \leq 2^{-N[T_\epsilon(\epsilon) - H(\epsilon)]}$$

$$\text{where } T_\epsilon(\epsilon) = -\epsilon \log_2 \epsilon - (1-\epsilon) \log_2 (1-\epsilon)$$

$$H(\epsilon) = -\epsilon \log_2 \epsilon - (1-\epsilon) \log_2 (1-\epsilon)$$

Let $\epsilon = \frac{1}{2}$. Then $T_{1/2}(\pi) = 1$ and inequality becomes

$$2^{-N} \sum_{i=0}^{\lfloor N\pi \rfloor} \binom{N}{i} \leq 2^{-N[1-H(\pi)]} \quad 0 \leq \pi \leq 1/2$$

$$\text{or } \frac{V}{\lfloor N\pi \rfloor} \leq 2^{N H(\pi)} \quad 0 \leq \pi \leq 1/2$$

From volume properties and letting $d_{\min} = N\pi$

$$V_{d_{\min}-1} \leq V_{d_{\min}} \leq 2^{N H\left(\frac{d_{\min}}{N}\right)}$$

for $0 \leq \frac{d_{\min}}{N} \leq 1/2$. Thus a code

with $d_{\min}$ and 2^K codewords exists if

$$2^{N H\left(\frac{d_{\min}}{N}\right)} \leq 2^{N-K} \quad 0 \leq \frac{d_{\min}}{N} \leq 1/2$$

$$\text{or } H\left(\frac{d_{\min}}{N}\right) \leq 1-R \quad 0 \leq \frac{d_{\min}}{N} \leq 1/2$$

see p. 50 of Peterson for plot of

$$1-H\left(\frac{d_{\min}}{N}\right) \text{ vs. } \frac{d_{\min}}{2N}$$

EX. Let $R = 1/2$, $H^{-1}(1/2) = 0.1100$

from Gilbert bound can find a code such that $\frac{d_{\min}}{N} \geq 0.1100$

so can correct $\sim 0.055 N$ errors

From Hamming bound

$$\frac{d_{\min}}{2N} < 0.1100$$

So can do no better than correct

0.11 N errors

Remark: Can always find a code as good as Gilbert bound. Can never find code better than Hamming Bound.

skip E. Plotkin Bound

(a) First step - bound on average distance of any block code of length N with M codewords

List of Code words

$$\vec{x}_1 = [x_{11}, x_{12}, \dots, x_{1N}]$$

$$\vec{x}_2 = [x_{21}, \dots, x_{2N}]$$

$\vdots$

$$\vec{x}_M = [x_{M1}, \dots, x_{MN}]$$

Let $n_j(x) =$ no. of codewords with x in j th position. Then $\vec{x}_1$ differs in j -th position from $M - n_j(x_{1j})$ codewords. Thus

$$\sum_{m=2}^M d(\vec{x}_1, \vec{x}_m) = \sum_{j=1}^N \{M - n_j(x_{1j})\}$$

$$\sum_{m \neq 1}^M d(\vec{x}_2, \vec{x}_m) = \sum_{j=1}^N \{M - n_j(x_{2j})\}$$

$$\sum_{n=1}^{M-1} d(\vec{x}_n, \vec{x}_m) = \sum_{j=1}^N \{M - n_j(x_{mj})\}$$

Now sum all terms

$$\sum_{m'=1}^M \sum_{\substack{n=1 \\ n \neq m'}}^M d(\vec{x}_{m'}, \vec{x}_n) = \sum_{j=1}^N \sum_{k=0}^{q-1} n_j(k) \{M - n_j(k)\}$$

since for each j on the right ~~hand~~ side of the set of M equations the quantity $M - n_j(k)$ occurs $n_j(k)$ times. Notice that $\sum_{k=0}^{q-1} n_j(k) = M$ for all j .

would like to pick $\{n_j(k)\}$ to maximize sum subject to this constraint. To do this need to maximize each term

$$\sum_{k=0}^{q-1} n_j(k) \{M - n_j(k)\} \quad j = 1, \dots, N$$

use Lagrange multiplier

$$\frac{\partial}{\partial n_j(k)} \left[\sum_{k=0}^{q-1} n_j(k) \{M - n_j(k)\} - \lambda \sum_{k=0}^{q-1} n_j(k) \right] = 0$$

$$M - 2n_j(k) - \lambda = 0$$

$$n_j(k) = \frac{M - \lambda}{2}$$

$$\sum_{l=0}^{q-1} n_j(l) = q \left(\frac{M-1}{2} \right) = M$$

$$\text{so } \frac{M-1}{2} = \frac{M}{q}$$

$$\text{and } n_j(l) = \frac{M}{q} \text{ for all } l \text{ and } j$$

Therefore

$$\sum_{m'=1}^M \sum_{\substack{m=1 \\ m \neq m'}}^M d(\vec{x}_{m'}, \vec{x}_m) \leq N q \frac{M}{q} \left(M - \frac{M}{q} \right) = NM^2 \frac{q-1}{q}$$

The number of terms ^{with $m' \neq m$} in the double summation is $M(M-1)$ so

$$d_{\text{avg}} = \frac{1}{M(M-1)} \sum_{m'=1}^M \sum_{\substack{m=1 \\ m \neq m'}}^M d(\vec{x}_{m'}, \vec{x}_m) \leq \frac{NM}{M-1} \frac{q-1}{q}$$

so

$$d_{\min} \leq d_{\text{avg}} \leq N \frac{M}{M-1} \frac{q-1}{q}$$

Remark: For (N, K) linear codes we proved

that $n_j(\alpha) = q^{K-1} = \frac{M}{q}$, so get equality

i.e.

$$d_{\text{avg}} = N \frac{q^{K-1}}{q^K - 1} (q-1)$$

as before.

alternate form of bound

$$(M-1) \frac{q}{q-1} d_{\min} \leq NM$$

$$\text{or } M \left(\frac{q}{q-1} d_{\min} - N \right) \leq \frac{q}{q-1} d_{\min}$$

so

$$\text{if } N < \frac{q}{q-1} d_{\min}$$

$$M \leq \frac{q d_{\min}}{q d_{\min} - N(q-1)}$$

(b) Second step - a fact about $A(N, d)$

Let $A(N, d)$ = number of codewords in that code of length N and $d_{\min} \geq d$ which has the most codewords. Take

$$A(N, d) = 1 \text{ for } N < d.$$

$$\text{since } \sum_{j=0}^{q-1} n_N(j) = M, \quad n_N(j) \geq M/q$$

for at least one j . Otherwise the sum would be less than M . Therefore at least M/q of the codewords agree in the last position. If a new code is formed by retaining only this set of code words, the minimum distance is not reduced. The last symbol ~~can~~ can be dropped without reducing

$d_{\min}$ since it is the same for all codewords.

Thus there is a code of length $N-1$ with at least M/q codewords. Therefore

$$A(N-1, d) \geq \frac{1}{q} A(N, d)$$

and repeating the argument i times

$$A(N, d) \leq q^i A(N-i, d)$$

→ (c) The bound (combining (a) and (b))

method is to shorten code so that

(a) gives good bound on M , then use (b) to extrapolate back to good bound at original length.

$$\text{Let } \frac{q d_{\min} - 1}{q - 1} = N' + r \quad \begin{array}{l} N' \text{ integer} \\ 0 \leq r < 1 \end{array}$$

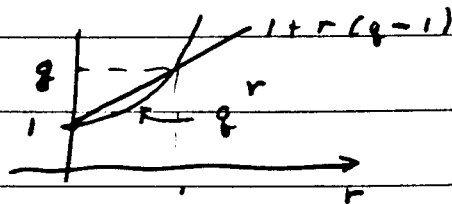
Thus $N' \leq q d_{\min} / (q - 1)$ so from (a)

$$A(N', d_{\min}) \leq \frac{q d_{\min}}{q d_{\min} - N'(q - 1)} = \frac{q d_{\min}}{1 + r(q - 1)}$$

$$\text{For } N \geq N' = \left\lfloor \frac{q d_{\min} - 1}{q - 1} \right\rfloor$$

$$\begin{aligned} A(N, d_{\min}) &\leq q^{N-N'} A(N', d_{\min}) \leq q^{N-N'+1} \frac{q d_{\min}}{1 + r(q - 1)} \\ &= d_{\min} \frac{q^{N - \frac{q d_{\min} - 1}{q - 1} + r + 1}}{1 + r(q - 1)} \end{aligned}$$

But $q^r \leq 1 + r(q-1)$ for $0 \leq r < 1$



Therefore

$$A(N, d_{\min}) \leq d_{\min} q^{N - \frac{q d_{\min}}{q-1} + \frac{q}{q-1}}$$

Thus for any code of length N with $d_{\min}$,

$$M = q^{NR} \leq A(N, d_{\min}) \leq q^{N - \frac{q d_{\min}}{q-1} + \frac{q}{q-1} + \log_q d_{\min}}$$

Take $\log_q$, rearrange

$$\frac{q}{q-1} \frac{d_{\min}}{N} - \frac{1}{N} \log_q d_{\min} \leq 1 - R + \frac{q}{N(q-1)}$$

$$\text{for } N \geq \left\lceil \frac{q d_{\min} - 1}{q-1} \right\rceil$$

Plotkin Bound

For fixed $R > 0$

$$\lim_{N \rightarrow \infty} \frac{d_{\min}}{N} \leq \frac{q-1}{q} (1-R)$$

Asymptotic Plotkin Bound

$$k \leq n - \frac{qd - 1}{q - 1} + 1 + \log_q d$$

This can be stated as follows:

Theorem 4.3. If $n \geq (qd - 1)/(q - 1)$, the number of check symbols required to achieve minimum weight d in an n -symbol linear code is at least $qd/(q - 1) - 1/(q - 1) - 1 - \log_q d$.

If d is very large, the last three terms in this expression are negligible. This bound is plotted for the binary case in Figure 4.1 with these three terms neglected.

The Plotkin bound can be proved for nonlinear codes also.

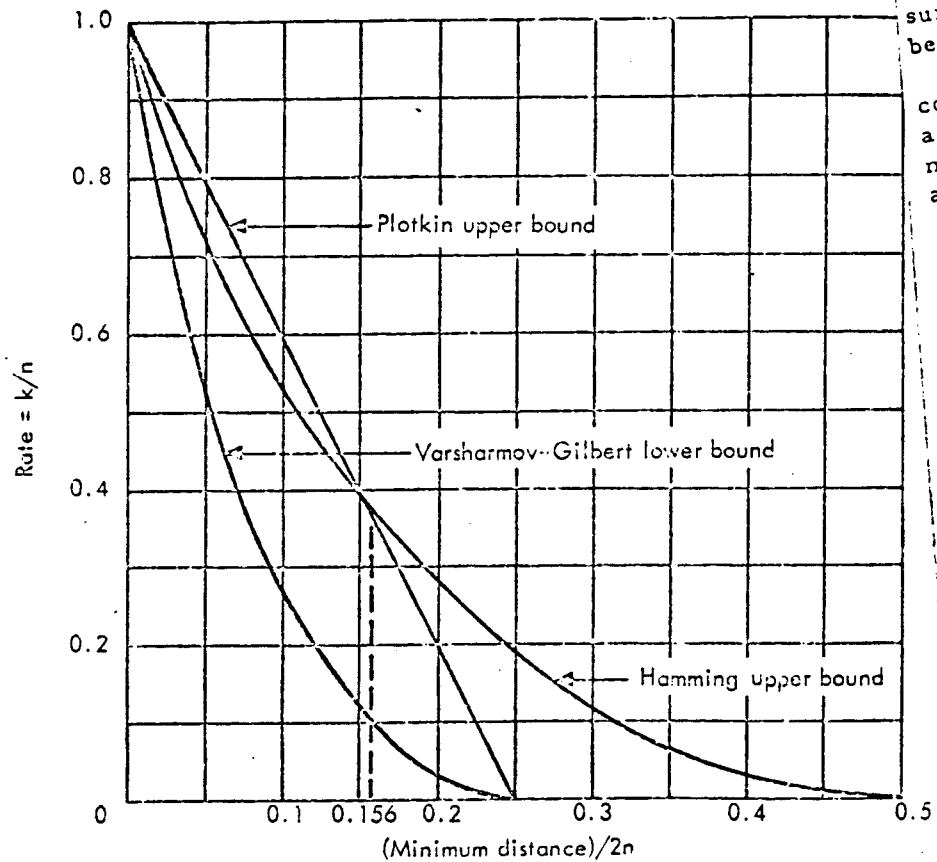


Figure 4.1. Bounds on minimum distance for the best code (the code length n is assumed to be very large)

2. The Varsharmov-Gilbert

By Theorem 3.1, if r is 1 or fewer columns, the matrix is a linear code. This suggests the following: if the first r columns of the parity-check matrix are linearly independent, then any nonzero r -tuple in the parity-check matrix is not a linear combination of the other columns. If a column is chosen as a linear combination of any $d - 2$ or fewer columns, it ensures that no linear combination of the other columns can be 0.

As long as the number of columns does not exceed $d - 1$, the columns added. In the worst case, the columns might be distinct, and thus there are

$$\binom{d-1}{1} (q-1)$$

linear combinations of the columns. If the number of columns is greater than $d - 1$, then the columns are linearly dependent.

$$\binom{n-1}{1} (q-1)$$

there exists a linear combination of the columns (and the minimum distance) that is 0.

Theorem 4.4. and minimum distance is at least

For large n , the minimum distance is approximately

EX: $R = 1/2$, $N = 100$, $q = 2 \Rightarrow d_{\min} \leq 25$

Comments: Plotkin's asymptotic bound tighter than Hamming bound for low rates, looser for high rates. Notice that $d/2N \approx t/N =$ fraction of correctable errors in block. For BSC with transition probability ϵ , the average number of errors is $N\epsilon$.

Let $r =$ number of errors that occur, then by Chebyshev's ineq.

$$P\left\{\left|\frac{r}{N} - \epsilon\right| \geq \alpha\right\} \leq \frac{\epsilon(1-\epsilon)}{N\alpha^2} \xrightarrow{N \rightarrow \infty} 0, \text{ so for large } N$$

the percentage of errors converges to ϵ with prob. 1. Thus by noisy coding Theorem, should be able to transmit error free at rate $R \leq C = 1 - H(t/N)$ which is Hamming Bound.

For $t/N > 0.156$ Plotkin Bound lower than Hamming Bound, $\Rightarrow$

apparent contradiction. Solution: The Plotkin bound guarantees can correct all patterns of t or fewer errors.

The code that achieves capacity can correct only most patterns of t or fewer errors.

F. Elias - Wyner Bound [Wyner, BSTJ 1965, pp. 1061-1122; Shannon, Gallager, Berlekamp, Info. + Control, 1968, pp. 522-552.]

Lemma 1

Let $A(N, d)$ be the same as defined above and let $\hat{A}(N, d, K)$ be the maximum number of codewords in a block code of length N with minimum distance $d_{\min}$ such that the weight of all codewords in the code is exactly K . Then $A(N, d) \leq \hat{A}(N, d, K) q^N / \left[\binom{N}{K} (q-1)^K \right]$.

Proof: Let $K \leq N$ and $\vec{y}$ an N -tuple over $GF(q)$. Define $u_K(\vec{y})$ as

$$u_K(\vec{y}) = \begin{cases} \frac{1}{\binom{N}{K}} & \text{if } w(\vec{y}) = K \\ 0 & \text{otherwise} \end{cases}$$

Let $\vec{x}_1, \dots, \vec{x}_M$ be a block code with minimum distance $d_{\min}$ and length N . With K fixed

for each N -tuple $\vec{y}$ define

$$u_k^*(\vec{y}) = \sum_{i=1}^M u_k(\vec{y} + \vec{c}_i)$$

Then
$$\sum_{\text{all } \vec{y}} u_k^*(\vec{y}) = \sum_{i=1}^M \sum_{\vec{y}} u_k(\vec{y} + \vec{x}_i)$$

$$= \sum_{i=1}^M \frac{1}{\binom{N}{k}} \{ \text{no. of } N\text{-tuples distance } k \text{ from } \vec{x}_i \}$$

$$= \sum_{i=1}^M \frac{1}{\binom{N}{k}} \binom{N}{k} (q-1)^k = M (q-1)^k \quad (1)$$

also

$$\sum_{\text{all } \vec{y}} u_k^*(\vec{y}) = \sum_{\text{all } \vec{y}} \sum_{i=1}^M u_k(\vec{y} + \vec{x}_i) \leq \sum_{\vec{y}} \max_{\vec{y}} \sum_{i=1}^M u_k(\vec{y} + \vec{x}_i)$$

let $\vec{y}_0$ achieve $\max_{\vec{y}} \sum_{i=1}^M u_k(\vec{y} + \vec{x}_i)$, then

$$\sum_{\vec{y}} u_k^*(\vec{y}) \leq q^N \sum_{i=1}^M u_k(\vec{y}_0 + \vec{x}_i) = q^N \frac{1}{\binom{N}{k}} \{ \text{no. of } \vec{x}_i \text{ such that } w(\vec{y}_0 + \vec{x}_i) = k \} \quad (2)$$

But $\vec{y}_0 + \vec{x}_1, \dots, \vec{y}_0 + \vec{x}_M$ has minimum distance $d_{\min}$, so that $\hat{A}(N, d_{\min}, k) \geq \{ \text{no. of } \vec{x}_i \text{ such that } w(\vec{y}_0 + \vec{x}_i) = k \}$

Combining (1) and (2)

$$M (q-1)^k \leq q^N \frac{1}{\binom{N}{k}} \hat{A}(N, d_{\min}, k)$$

or
$$A(N, d) \leq \frac{q^N}{(q-1)^k} \frac{1}{\binom{N}{k}} \hat{A}(N, d_{\min}, k)$$

Q.E.D.

Lemma 2.

$$\hat{A}(N, d_{\min}, K) \leq \frac{d_{\min}}{d_{\min} - 2K(1 - \frac{K}{N} \frac{q}{q-1})}$$

if denominator is positive.

Proof: Consider an N dimensional code with minimum distance $d_{\min}$, code words

$\vec{x}_1, \dots, \vec{x}_{\hat{A}}$ such that $w(\vec{x}_i) = K$ for $i = 1, \dots, \hat{A}$. Then from Plotkin bound

proof:

$$\begin{aligned} \hat{A}(\hat{A}-1) d_{\min} &\leq \sum_{m'=1}^{\hat{A}} \sum_{\substack{m=1 \\ m \neq m'}}^{\hat{A}} d(\vec{x}_m, \vec{x}_{m'}) \\ &= \sum_{j=1}^N \sum_{k=0}^{q-1} n_j(k) \{ \hat{A} - n_j(k) \} \\ &= \frac{1}{\hat{A}} \sum_{j=1}^N \sum_{k=1}^{q-1} n_j(k) + \frac{1}{\hat{A}} \sum_{j=1}^N n_j(0) - \sum_{j=1}^N \sum_{k=1}^{q-1} n_j^2(k) \\ &\quad - \sum_{j=1}^N n_j^2(0) \end{aligned}$$

But

(a) $\sum_{j=1}^N \sum_{k=1}^{q-1} n_j(k) = \hat{A} K$ since there are $\hat{A}$ codewords of weight K

(b) $\sum_{j=1}^N n_j(0) = \hat{A} (N-K)$ - number of 0's in all $\hat{A}$ codewords

(c) bound on third term

By Schwarz's inequality

$$\left(\sum_{j=1}^N \sum_{k=1}^{q-1} n_j(k) \right)^2 \leq \left[\sum_{j=1}^N \sum_{k=1}^{q-1} n_j^2(k) \right] \left[\sum_{j=1}^N \sum_{k=1}^{q-1} (1)^2 \right]$$

$$\text{or } (\hat{A} K)^2 \leq \left[\sum_{j=1}^N \sum_{k=1}^{q-1} n_j^2(k) \right] N(q-1)$$

$$\text{or } \sum_{j=1}^N \sum_{k=1}^{q-1} n_j^2(k) \geq \frac{(\hat{A} K)^2}{N(q-1)}$$

(d) Bound on 4^{th} term

$$\left[\sum_{j=1}^N n_j(0) x_1 \right]^2 \leq N \sum_{j=1}^N n_j^2(0)$$

$$\text{or } \sum_{j=1}^N n_j^2(0) \geq \frac{[\hat{A}(N-K)]^2}{N}$$

Combining all these results gives

$$\begin{aligned} \hat{A}(\hat{A}-1) d_{\min} &\leq \hat{A}^2 K + \hat{A}^2 (N-K) + \frac{\hat{A}^2 K^2}{N(q-1)} - \frac{\hat{A}^2 (N-K)^2}{N} \\ &= \hat{A}^2 K - \frac{\hat{A}^2 K^2 q}{N(q-1)} \end{aligned}$$

Q.E.D.

The Bound: Combining Lemmas 1 and 2

$$M \leq A(N, d) \leq \min_K \frac{q^N}{\binom{N}{K} (q-1)^K} \left[\frac{d_{\min}}{d_{\min} - 2K + \frac{K^2 q}{N(q-1)}} \right]$$

provided that the denominator is positive

Asymptotic Bound

let K be smaller root of

$$d_{\min} - 2K + \frac{K^2 q}{N(q-1)} = 1$$

i.e.

$$R = \frac{q-1}{q} N \left[1 - \sqrt{1 - \frac{q}{q-1} \frac{d_{\min}-1}{N}} \right]$$

So that

$$M \leq \frac{q^N d_{\min}}{\binom{N}{k} (q-1)^k}$$

For $q=2$

$$\frac{R}{N} = \frac{1}{2} - \frac{1}{2} \sqrt{1 - 2 \frac{d_{\min}}{N}} + O_1(N)$$

where $\lim_{N \rightarrow \infty} O_1(N) = 0$, From Hamming bound

$$\binom{N}{k} \leq 2^{N[H(\frac{k}{N}) + O_2(N)]}$$

also

$$d_{\min} = 2^{\log_2 d_{\min}} = 2^{N O_3(N)}$$

So

$$M = 2^{NR} \leq q^{N[1 - H(\frac{k}{N}) + O_3(N)]}$$

and for $R > 0$ and fixed

$$\lim_{N \rightarrow \infty} H\left(\frac{1}{2} - \frac{1}{2} \sqrt{1 - 2 \frac{d_{\min}}{N}}\right) \leq 1 - R$$

Elias Asymptotic Bound

Superior to Plotkin + Hamming Bounds
Table of Values (add to 1.50 Peterson)

$d_{\min}/N$	0	.100	.200	.300	.400	.500
R	1	.701	.491	.311	.151	0