1. Bounds for Code parameters

We have identified this far three important parameters for q-block codes: the length n, the size M and the distance d. We will refer from now on to (n, M, d)-codes, in order to specify the parameters. In the case of a linear code, the size is $M = q^k$, where k is the dimension of the code, as a $\mathbb{F}_q$ vector space; we'll refer to $[n, k]$-linear codes or $[n, k, d]$-linear codes when the distance is specified.
These parameters are not completely independent. They satisfy inequalities that establish bounds for one of them depending on the others.
We consider in particular bounds on M depending on n and d and define

1. $A_q(n, d)$ is the maximum possible size M such that a code of length n and minimum distance at least d exists;
2. $B_q(n, d)$ is the maximum possible size M such that a linear code of length n and minimum distance at least d exists; in this case $M = q^k$, where k is the dimension of the code.

Naturally, $B_q(n, d) \leq A_q(n, d)$ for every n and d. It is also clear that to prove that $A_q(n, d) \geq L$ we must show the existence of a code with length n, with size at least L and minimum distance at least d. On the other hand, to prove that $A_q(n, d) \leq L$ we must show that any code with length n and minimum distance at least d has size at most L.

Let $N(u, r)$ be the sphere of radius r around $u \in \mathbb{F}_q^n$, ie, $N(u, r) = \{x \in \mathbb{F}_q^n : \text{dist}(u, x) \leq r\}$. We define

- $t = \lfloor \frac{d-1}{2} \rfloor$ as the **packing radius** of C; it is the largest r such that for all distinct codewords c and c', $N(c, r) \cap N(c', r) = \emptyset$.
- $\text{cov}(C)$ is the **covering radius** of C; it is the least r such that $\mathbb{F}_q^n = \cup_{c \in C} N(c, r)$.

Exercise 1. $\text{cov}(C) = \max_{x \in \mathbb{F}_q^n} \min_{c \in C} \text{dist}(x, c)$.

We recall also the characterization of $\text{cov}(C)$ for linear codes:

Lemma 2. *The covering radius of a linear code C is equal to*

i) $\max\{i : \alpha_i > 0\}$, *where α_i denotes the number of unique coset leaders with weight i;*
ii) *the smallest integer s such that any $v \in \mathbb{F}_q^{n-k}$ is a linear combination of some s columns of the parity check matrix of C.*

A simple counting argument shows that (independently of the vector u)

$$V_q(n, r) = |N_q(u, r)| = \begin{cases} \sum_{i=0}^{r} \binom{n}{i} (q-1)^i & r < n \\ q^n & n \leq r \end{cases}$$

1.1. **The Sphere-covering bound.** Suppose C is an optimal (n, M, d)-code with respect to M, ie, the size M of C satisfies $M = A_q(n, d)$. We must then have

$$\forall v \in \mathbb{F}_q^n \ \exists c \in C : d(v, c) < d,$$

because otherwise a vector v could be added to C. This implies that $\mathrm{cov}(C) \leq d-1$, ie

$$\mathbb{F}_q^n = \bigcup_{c \in C} N(c, d-1).$$

So

$$q^n \leq MV_q(n, d-1).$$

Notice that the same argument applies for a linear code. We conclude that

Proposition 3. *Given fixed n and d,*

$$\frac{q^n}{V_q(n, d-1)} \leq B_q(n, d) \leq A_q(n, d).$$

1.2. **The Sphere Packing bound (or Hamming bound).** The Hamming bound provides, on the other hand, an upper bound on the distance or on the size of a code. We present two versions with two different proofs.

Proposition 4. *If C is a $[n, k]$-linear code that is t-error correcting, then*

$$V_q(n, t) \leq q^{n-k}.$$

Proof. Recall that a linear code is t-error correcting iff all vectors v with $w(v) \leq t$ are coset leaders.
The number of cosets is q^{n-k} while the left-hand side in the inequality counts the number of vectors v with $w(v) \leq t$. □

Because a code is t-error correcting iff it satisfies $t \leq \frac{d-1}{2}$, this inequality establishes an upper bound for the distance of any $[n, k]$-linear code. But, fixing n and d, we obtain also an upper bound on $B_q(n, d)$:

$$B_q(n, d) \leq \frac{q^n}{V_q(n, t)}$$

The same bound holds for general block codes, by a reasoning similar to the one used for the proof of the sphere-covering bound:
Suppose that C is an optimal (n, M, d)-code with respect to M, ie, $M(C) = A_q(n, d)$. Denote $t = \left\lfloor \frac{d-1}{2} \right\rfloor$; the spheres $N(c, t)$, where $c \in C$, are disjoint; using the formula for $|N(c, t)|$, we obtain

$$MV_q(n, t) \leq q^n$$

and so

Proposition 5.

$$A_q(n, d) \leq \frac{q^n}{V_q(n, t)}.$$

Definition 6. *If n, M and d satisfy $MV_q(n, t) = q^n$, with $t = \left\lfloor \frac{d-1}{2} \right\rfloor$, a (n, M, d)-code is called* ***perfect****.*

So in a perfect code the spheres $N(c,t)$ form a partition of the space $\mathbb{F}_q^n$ and the packing and covering radius coincide.

Exercise 7. *Show that a perfect t-error-correcting linear code of length n over $\mathbb{F}_q$ has exactly $\binom{n}{i}$ cosets with coset leader of weight i, for $0 \leq i \leq t$ and no other cosets.*

Example 8. *The following are the* ***trivial perfect codes****:*

i) $C = \mathbb{F}_q^n$*;*
ii) *codes with size* 1*;*
iii) *binary repetition codes of odd length;*
iv) *binary codes of odd length consisting of one vector c and its complementary vector c' (c with the* 0*s and* 1*s interchanged).*

Non-trivial examples of perfect codes are given, as seen before, by the Hamming codes. Other important examples are the $[23, 12, 7]$ binary and $[11, 6, 5]$ ternary Golay codes. In fact, these examples essentially cover all non-trivial perfect codes, which are completely classified in the following theorem, quoted without proof:

Theorem 9. 1- *The only linear single error-correcting perfect codes over a field $\mathbb{F}_q$ are the Hamming codes. There exist nonlinear perfect single error-correcting codes over $\mathbb{F}_q$ and they have the same parameters (length, size and minimal distance) of the Hamming codes over the same field.*

2- *The only nontrivial multiple error-correcting perfect codes have the same parameters as one of the two Golay codes, and any binary (respectively, ternary) code of size 2^{12} (respectively, 3^6), length* 23 *(respectively,* 11*) and minimal distance* 7 *(respectively,* 5*), containing the zero vector, is equivalent to the binary $[23, 12, 7]$ (respectively, ternary $[11, 6, 5]$) Golay code.*

Remark 10. *Aa code with packing radius t and covering radius $t + 1$ is called* ***quasi-perfect****. Although there are examples of both linear and nonlinear quasi-perfect codes, no general classification is known.*

1.3. **Inequalities in the $A_q(n, d)$ and $B_q(n, d)$ sequences.** Before we proceed with the study of other bounds, we notice some basic but useful inequalities.

Proposition 11. *For all positive n and d,*

$$A_q(n, d+1) \leq A_q(n, d) \leq A_q(n+1, d), \qquad B_q(n, d+1) \leq B_q(n, d) \leq B_q(n+1, d).$$

Proof. This is an immediate consequence of the definitions (**HW**). □

Proposition 12. *If $d > 1$,*

$$A_q(n, d) \leq A_q(n-1, d-1), \qquad B_q(n, d) \leq B_q(n-1, d-1).$$

Moreover, if $q = 2$ and d is even

$$A_2(n, d) = A_2(n-1, d-1), \qquad B_2(n, d) = B_2(n-1, d-1).$$

Proof. If C is a (n, M, d) code over $\mathbb{F}_q$, the code $C^{[i]}$, ie the puncturing of C at the coordinate i, is a $(n-1, M, d')$ code, with $d' \geq d-1$: there is not a pair of codewords differing only at i, because $d > 1$. So, by definition, $M \leq A_q(n-1, d-1)$; if we take $M = A_q(n, d)$ we obtain the result. The argument for linear codes is identical and left as an exercise.
For the proof of the second part, and in view of the inequality already proved, it suffices to show that if C is a $(n-1, M, d-1)$ binary code, with d even, and $M = A_2(n-1, d-1)$, there exists a (n, M, d) code. Consider the extension $\hat{C}$ of C by parity-checking, ie

$$\hat{C} = \{\hat{c} = (c_1, \cdots, c_{n-1}, c_n) \in C \times \mathbb{F}_2 : \sum_i c_i = 0\}.$$

Suppose that $x = (x_1, \cdots, x_{n-1})$ and $y = (y_1, \cdots, y_{n-1})$ are two codewords of C at distance $d-1$; we verify that, because d is even, one of the two has even weight while the other has odd weight (**HW**); so in the extended code, the entries x_n and y_n of $\hat{x}$ and $\hat{y}$ will be different, implying that $\text{dist}(\hat{x}, \hat{y}) = d$. □

Remark 13. *The equalities in the second part show that, for binary codes, it is sufficient to know the values $A_2(n, d)$ or $B_2(n, d)$ for all even d or for all odd d.*

Example 14. *Let $q = 2$, $n = 14$ and $d = 6$. The direct application of the Hamming bound implies that $A_2(14, 6) \leq 154$. However, a similar computation gives $A_2(13, 5) \leq 89$.*

Proposition 15.

$$A_q(n, d) \leq qA_q(n-1, d), \qquad B_q(n, d) \leq qB_q(n-1, d).$$

Proof. (**HW**): Let C be a (n, M, d) code with $M = A_q(n, d)$, and, for each $a \in \mathbb{F}_q$, let

$$C(a) = \{c \in C : c_n = a\}.$$

Show that, for some a, the punctured code $(C(a))^{[n]}$ has at least M/q codewords and minimal distance d.
For the proof of the second inequality, consider a $[n, k, d]$ code C, and show that, for any fixed coordinate i, the set of codewords c with $c_i = 0$ is either C or a $[n, k-1, d]$ code. □

1.4. **The Varshamov bound.** We obtain now a bound for linear codes:

Proposition 16. *Let $2 \leq d \leq n$ and $1 \leq k \leq n$. If*

$$V_q(n-1, d-2) < q^{n-k}$$

then there exists a $[n, k]$-linear code C such that $d(C) \geq d$.

Proof. We show that, for any $1 \leq l \leq n$, there exists a $(n-k) \times l$ matrix such that any $d-1$ columns are linearly independent: the claim is certainly true for $l = 1$, as we may choose any non-zero $(n-k)$ vector; assume the claim is true for $j < n$; the number of linear combinations of at most $d-2$ of the j columns is

$$V_q(j, d-2) \leq V_q(n-1, d-2) < q^{n-k};$$

so it is possible to choose a vector that is linearly independent of any already chosen $d-2$ columns, thus completing the induction step.
This sum includes, for $i = 0$, the zero vector as a linear combination of an empty set of vectors; alternatively, we could write the condition as $\sum_{i=1}^{d-2} \binom{n-1}{i}(q-1)^i < q^{n-k} - 1$; in the induction step this means that we can choose a non-zero vector.

By eliminating eventual linear dependences on the rows, we get a $m \times n$ matrix which is a parity-check matrix for a code C' with length n, distance at least d and dimension $n - m \geq k$; choosing a k-dimensional subspace we obtain the desired $[n, k]$-linear code C with $d(C) \geq d$, as the minimum distance of a subspace C must be greater or equal than the minimum distance of C'. □

The result may be interpreted as a lower bound for the maximal distance of a $[n, k]$-linear code, for fixed n and k, but also as a lower bound for $B_q(n, d)$.

Exercise 17. *Determine the lower bound for $B_q(n, d)$ implied by Varshamov's bound.*

1.5. **Singleton Bound and MDS Codes.** We obtain another upper bound on the size of codes: let C be a (n, M, d) code; if we puncture C at some $d-1$ coordinates, we are left with M *distinct* vectors from $\mathbb{F}_q^{n-(d-1)}$. So $M \leq q^{n-d+1}$.
We may apply this reasoning to $[n, k, d]$ linear codes and conclude that $k \leq n-d+1$.

Despite its simplicity, there exist codes attaining the Singleton bound: a (n, M, d) code such that $M = q^{n-d+1}$ is called a **Maximum Distance Separated (MDS)** code.
We prove a few useful results about MDS codes.

Lemma 18. *If C is a $[n, k, d]$ code over some $\mathbb{F}_q$, any set of $n-d+1$ coordinates contains an information set.*

Proof. Suppose that a set S of s coordinates does not contain an information set and let B be the corresponding $k \times s$ submatrix of a generator matrix G. Then B has rank $< k$ and so the zero vector is a non-zero linear combination of the rows of B; this means that there exists some $c \in C$ with $\mathrm{supp}(c) \subset [n] \setminus S$, which implies that $n - s \geq d$, ie, $s \leq n - d$. □

Corollary 19. *C is MDS if and only if any set of k coordinates is an information set.*

Proof. **HW**. □

Proposition 20. *The dual of a MDS code is also MDS: if C is a $[n, k, n-k+1]$ over $\mathbb{F}$, then $C^\perp$ is a $[n, n-k, k+1]$ code.*

Proof. This is a consequence of the previous corollary once we notice that a $S \subset [n]$ is an information set for C if and only if $[n] \setminus S$ is an information set for $C^\perp$ (**HW**). □

Proposition 21. *If C is a $[n, k, n-k+1]$ code over F, then its shortening $C_{[i]}$ at the i coordinate is a $[n-1, k-1, n-k+1]$ code.*

Proof. $\dim(C_{[i]}) = \dim(C(i))$ where $C(i) = \{c \in C : c_i = 0\}$. Being the kernel of a linear map from C to $\mathbb{F}$, $C(i)$ has dimension either k or $k-1$, and the first case occurs exactly if $c_i = 0$ for all $c \in C$; but, by the above Lemma, this can not happen for a MDS code.
The distance d' of $C_{[i]}$ satisfies $d' \geq d$ (**HW**); but the Singleton bound implies that $d' \leq n - 1 - (k-1) + 1 = d$. □

1.6. **Residual Codes and Griesmer Bound.** Let C be a $[n, k, d]$ code over $\mathbb{F}_q$ and suppose $c \in C$ satisfies $w(c) = d$. Without loss of generality (ie, by taking an equvalent code) we may assume, for simplicity, that the support of c consists on the first d coordinates and that $c_i = 1$ for every $i \in \mathrm{supp}(c)$. Define $Res(C, c)$ to be the puncturing of C on $\mathrm{supp}(c)$. It is a $[n-d, k', d']$ linear code with $k' < k$ (it contains less than q^k vectors).
If $k' < k-1$ then there would exist $x \in C$, not a multiple of c, such that $\mathrm{supp}(x) = \mathrm{supp}(c)$ (**HW**); but then there exists $a \in \mathbb{F}_q \setminus \{0\}$ such that $x_i = a$ for at least $\lceil d/(q-1) \rceil$ of the first d coordinates; so

$$d \leq w(x - ac) \leq d - \lceil d/(q-1) \rceil \leq d\frac{q-2}{q-1} < d,$$

a contradiction. So $k' = k-1$.
As to the value of d', let $x \in C$ such that its puncturing $x' \in Res(C, c)$ is not zero; the same reasoning as before gives

$$d \leq w(x - ac) \leq d - \lceil d/q \rceil + w(x'),$$

ie

$$w(x') \geq \lceil d/q \rceil .$$

In particular, we obtained

Proposition 22. *If C is a $[n, k, d]$ code over $\mathbb{F}_q$ and $c \in C$ satisfies $w(c) = d$ then $Res(C, c)$ is a $[n-d, k-1, d']$ code with $d' \geq \lceil d/q \rceil$.*

Example 23. *Suppose C is a $[16, 8, 6]$ binary code (notice that these values are not ruled out by the Hamming or Singleton bounds). Taking c with $w(c) = 6$, $Res(C, c)$ would be a $[10, 7, d]$ code with $d \geq 3$ but this is impossible: just examine a possible generator matrix $G = [I|A]$ for C (or eventually an equivalent code) (**HW**). So C does not exist.*

We now use the previous result to deduce a new bound:

Proposition 24 (Griesmer Bound)**.** *If C is a $[n,k,d]$ code over $\mathbb{F}_q$*

$$\sum_{i=0}^{k-1}\left\lceil\frac{d}{q^i}\right\rceil\leq n.$$

Proof. We prove the inequality

$$\sum_{i=0}^{j-1}\left\lceil\frac{d}{q^i}\right\rceil\leq n.$$

holds for $j\leq k$ by induction: for $j=1$ it reduces to $d\leq n$; assuming it holds for $j<k$, and puncturing C at $\mathrm{supp}(c)$ for some c satisfying $w(c)=d$, we get $Res(C,c)$; by induction hypotthesis

$$n-d\geq\sum_{i=0}^{k-2}\left\lceil\frac{d'}{q^i}\right\rceil\geq\sum_{i=0}^{k-2}\left\lceil\frac{d}{q^{i+1}}\right\rceil,$$

as a consequence of th previous proposition.
This implies that

$$n\geq d+\sum_{i=1}^{k-1}\left\lceil\frac{d}{q^i}\right\rceil=\sum_{i=0}^{k-1}\left\lceil\frac{d}{q^i}\right\rceil.$$

□

Exercise 25. *Let C be the dual of the r-dimensional Hamming code over $\mathbb{F}_q$. Show that every nonzero codeword of C has weight q^{r-1} and that C meets the Griesmer bound.*

In fact, we have

Theorem 26. *Let C be a $[n,k,d]$ binary code that meets the Griesmer bound. Then C has a basis of minimum weight codewords.*

Proof. We sketch the proof leaving the details to the reader. The proof is by induction on k, the case $k=1$ being trivial (**HW**). Let $c\in C$ be a codeword of minimal weight; we may assume (why?) that the nonzero coordinates are the first d and that C has a generator matrix

$$G=\left[\begin{array}{c|c}1\cdots1&0\cdots0\\\hline G_0&G_1\end{array}\right]$$

Claim 27. *Let $d_1=\lceil d/2\rceil$; for any $i\geq1$ we have*

$$\left\lceil\frac{d}{2^i}\right\rceil=\left\lceil\frac{d_1}{2^{i-1}}\right\rceil.$$

Claim 28. *The residual code $Res(C,c)$ is a $[n-d,k-1,d_1]$ code and so meets the Griesmer bound.*

By induction, we may assume that the rows of G_1 above have weight d_1. Let $r=(u,v)$ denote a row of G, other than the first, where u is a row of G_0 and v a row of G_1.

Claim 29. *Either r or $c+r$ has weight d and so C has a basis of codewords with weight d.*

□

Exercise 30. *Complete the proof of the theorem.*

1.7. **Asymptotic Bounds.** There are many other general bounds for $A_q(n,d)$, some of them with rather complicated definitions. And for concrete n and d it is possible to strengthen those bounds and sometimes even to establish the exact value of $A_q(n,d)$. However these numbers remain undetermined even for some relatively small values of the parameters. As an example, we present the current (as far as I know) known bounds for a couple of concrete cases:

$$2720 \leq A_2(17,4) \leq 3276, \qquad 256 \leq A_2(17,6) \leq 340,$$

and maybe even more impressive,

$$36 \leq A_2(17,8) \leq 37.$$

A different approach consists in trying to predict the asymptotitc behaviour of those numbers, as n grows. In that case, we try to bound not the size M of the codes as a function of n and d, but the information rate as a function of n and of d/n.

Definition 31. *For $0 < \delta < 1$, let*

$$\alpha_q(\delta) = \limsup_n \frac{\log_q(A_q(n,\delta n))}{n}.$$

We have obviously $0 \leq \alpha_q(\delta) \leq 1$.
If $\alpha_q(\delta) < t$, for any family C_n of codes over $\mathbb{F}_q$, where C_n is a (n, M_n, d_n) code such that $\frac{d_n}{n} \geq \delta$, we know that, for sufficiently large n, $M_n < q^{nt}$. On the other hand, if $s < alpha_q(\delta)$, then we know that there exists such a family satisfying, again for sufficiently large n, $q^{ns} < M_n$.

Asymptotic bounds are derived from bounds for $A_q(n,d)$. The simplest example is

Proposition 32 (Singleton asymptotic bound)**.** *For any q, $\alpha_q(\delta) \leq 1 - \delta$.*

Proof. (**HW**). This is a direct consequence of the Singleton bound. □

For a more interesting example (and also a better asymptotic bound), we deduce the aymptotic version of the **Plotkin bound**: let $\theta = \frac{q-1}{q}$; then, if C is a (n, M, d) code over $\mathbb{F}_q$, and $d \geq \theta n$, we have

$$M \leq \left\lfloor \frac{d}{d - \theta n} \right\rfloor.$$

We fix q and suppose first that $\delta > \theta$. Then the minimal distance of a $(n, M, \delta n)$ code satisfies $d > \theta n$ and, by Plotkin bound,

$$A_q(n, \delta n) \leq \frac{\delta n}{\delta n - \theta n},$$

and so (**HW**)

$$\alpha_q(\delta) = 0.$$

So, for a family of arbitrarily long codes with $d/n > \theta$ the information ratio will inevitably tend to zero.

On the other hand, if $\delta \leq \theta$ the Plotkin bound can not be directly applied. Let C be a $(n, M, \delta n)$ code over $\mathbb{F}_q$ for which $M = A_q(n, \delta n)$. We notice that

$$m = \left\lfloor \frac{\delta n - 1}{\theta} \right\rfloor < n$$

and that (**HW**) there exists $a_1, \cdots, a_{n-m}$ such that at least M/q^{n-m} code words c satisfy $c_i = a_i$, for $1 \leq i \leq n - m$. Puncturing in the first $n - m$ coordinates the subcode of C constitude by those codewords, we obtain a $(m, M', \delta n)$ code C', with $M' \geq M/q^{n-m}$. The choice of m implies that $\delta n - \theta m \geq 1$; in particular, we may apply Plotkin's bound to C' and we get

$$\frac{M}{q^{n-m}} \leq M' \leq \frac{\delta n}{\delta n - \theta m} \leq \delta n,$$

implying that (**HW**)

$$\alpha_q(\delta) \leq 1 - \frac{\delta}{\theta}.$$

We proved

Proposition 33 (Asymptotic Plotkin bound)**.** *If* $\theta = \frac{q-1}{q}$,

$$\begin{cases} \alpha_q(\delta) = 0 & \text{if } \delta > \theta \\ \alpha_q(\delta) \leq 1 - \frac{\delta}{\theta} & \text{if } \delta \leq \theta \end{cases}$$

2. Supplementary Results and Problems

Problem 34. *Reprove the Sphere-covering Bound for linear codes, in the following form: if*

$$\sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i < q^{n-k+1},$$

then there exists a $[n, k, d]$ *code over* $\mathbb{F}_q$.

Problem 35. *Compare the different upper bounds on* k *for binary* $[15, k, 5]$*-linear codes and determine* $B_2(15, 5)$.

Problem 36. *Let* C *be a* $[n, k, d]$*-linear code over* $\mathbb{F}_q$ *such that for every* $1 \leq i \leq n$ *there exists a codeword* $c = (c_1, \cdots, c_n)$ *with* $c_i \neq 0$.

a) *Show that* $\sum_{c \in C} w(c) = n(q-1)q^{k-1}$;

b) *Show that* $d \leq \frac{n(q-1)q^{k-1}}{q^k - 1}$;

c) *Show that there cannot be a binary* $[15, 7, d]$*-linear code for* $d > 7$.

Hint: *Consider the table whose rows are the codewords and compute the sum of the weights in two ways.*

Problem 37 (The binary **Plotkin bound**). *Let C be a binary $[n,k,d]$-linear code.*

a) *Show that the number of codewords that have a 0 at position j is either 2^k or 2^{k-1};*
b) *Show that $\sum_{c\in C} w(c) \leq n2^{k-1}$;*
c) *Prove that $d \leq \frac{n2^{k-1}}{2^k-1}$.*

Problem 38 (**Plotkin bound**: general case). *Suppose C is a (n,M,d) code over $\mathbb{F}_q$. Consider the table whose rows are the codewords and, for a given fixed column, denote by m_j the number of ocurrences of $j \in \mathbb{F}_q$ in that column.*
Denote by S the sum of distances between distinct codewords: $S = \sum_{c\neq c'} \mathrm{dist}(c,c')$.

a) *Verify that the contribution of the fixed column to S is*

$$\sum_{j\in\mathbb{F}_q} m_j(M-m_j) = M^2 - \sum_{j\in\mathbb{F}_q} m_j^2 \leq \theta M^2$$

where $\theta = \frac{q-1}{q}$.
Hint: *Apply Cauchy-Schwarz inequality to $\sum_j m_j$.*
b) *By summing over all ordered pairs of codewords, conclude that*

$$M(M-1)d \leq n\theta M^2 \Leftrightarrow d \leq n\theta\frac{M}{M-1}.$$

Problem 39. *Let C be the dual code of the $[13,10,3]$ Hamming code over $\mathbb{F}_3$. Verify that C satisfies Plotkin bound with equality.*

2.1. **Linear codes with minimal weight basis and codes of constant weight.** In conection with the results at the end of the section about the Griesmer bound, we have

Theorem 40. *Suppose that C is a $[n,k,d]$ code over $\mathbb{F}_q$. Then there exists also a code with the same parameters over the same field with a basis of minimal weight codewords.*

Problem 41. *Prove the theorem: Suppose that $c_1,\cdots,c_s$ is a maximal linearly independent set of codewords of C with weight d, and that $s<k$. Denote as S the span of this family of codewords. Let*

$$\{c_1,\cdots,c_s,e_1,\cdots,e_{k-s}\}$$

be a basis of C such that e_1 has minimal weight $d_1 > d$ among the vectors of $C\setminus S$; choose d_1-d nonzero coordinates of e_1 and let e be the vector obtained from e_1 by replacing those coordinates by zero.
Show that the space generated by the given basis of C with e_1 replaced by e is a $[n,k,d]$ code.
Deduce the statement of the theorem.

Problem 42. *Let C be the binary code with generator*

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

Show that C has minimal distance 4.
Apply the proof of the theorem to construct a $[9, 4, 4,]$ code with a basis of minimal weight vectors.

Codes with constant weight (necessarily nonlinear) are interesting on their own and have a role in the deduction of certain bounds. Denote by $A_q(n, d, w)$ the maximal possible size of a code over $\mathbb{F}_q$ with length n, minimal distance at least d and constant weight w.

Problem 43. *Prove the following bounds:*

i) *If $d > 2w$ then $A_q(n, d, w) = 1$;*
ii) $A_q(n, d, w) \leq \left\lfloor \frac{n(q-1)}{w} \right\rfloor$;
iii) $A_2(n, 2w, w) = \lfloor n/w \rfloor$;
iv) $A_2(n, 2e - 1, w) = A_2(n, 2e, w)$.

Bounds for constant weight codes are also a tool to prove general bounds. A preparation for the Johnson bound (not presented in these notes) are the following

Theorem 44 (Restricted Johnson Bound)**.** *If $qw^2 - 2(q-1)nw + nd(q-1) > 0$,*

$$A_q(n, d, w) \leq \left\lfloor \frac{nd(q-1)}{qw^2 - 2(q-1)nw + nd(q-1)} \right\rfloor.$$

Problem 45. *Prove the theorem: Let C be a (n, M, d) code with constant weight w; consider the $M \times n$ matrix L with all codewords as rows and let $S = \sum_{x \in C} \sum_{y \in C} \operatorname{dist}(x, y)$.*

a) *Prove that $M(M-1)d \leq S$.*
b) *Denoting as $n_{i,a}$ the number of times that $a \in \mathbb{F}_q$ occurs in the i-th column of L, show that*

$$S = \sum_{i=1}^{n} \sum_{a \in \mathbb{F}_q} n_{i,a}(M - n_{i,a}) =$$

$$= \sum_{i=1}^{n} (M n_{i,0} - n_{i,0}^2) + \sum_{i=1}^{n} \sum_{a \in \mathbb{F}_q^\times} n_{i,a}(M - n_{i,a}),$$

where $\mathbb{F}_q \times = \mathbb{F}_q \setminus \{0\}$.
c) *Show that $\sum_{i=1}^{n} n_{i,0} = (n-w)M$ and, using the Cauchy-Schartz inequality*

$$\sum_{i=1}^{n} \sum_{a \in \mathbb{F}_q} n_{i,a}(M - n_{i,a}) \leq (n-w)M - \frac{(n-w)^2 M^2}{n}.$$

d) *Prove, similarly, that $\sum_{i=1}^{n} \sum_{a \in \mathbb{F}_q^\times} n_{i,a} = wM$ and that*

$$\sum_{i=1}^{n} \sum_{a \in \mathbb{F}_q^\times} n_{i,a}(M - n_{i,a}) \leq wM^2 - \frac{w^2 M^2}{n(q-1)}.$$

e) *Deduce the theorem.*

Problem 46. *Suppose $d \leq 2w$ and let C be a (n, M, d) code over $\mathbb{F}_q$ of constant weight w, and such that $M = A_q(n, d, w)$.*
Let, as above, L be the $M \times n$ matrix with all codewords as rows.

a) *For each* $a \in \mathbb{F}_q^\times$, *let* $C_i(a)$ *be the subcode whose codewords have* a *in the* i*-th coordinate and put* $m_{i,a} = |C_i(a)|$. *Show that*

$$\sum_{a\in\mathbb{F}_q^\times} \sum_{i=1}^{n} m_{i,a} = wM.$$

b) *Verify that the puncturing* $(C_i(a))^{[i]}$ *is a* $(n-1, m_{i,a}, d)$ *code of constant weight* $w-1$, *and deduce that*

$$A_q(n,d,w) \le \left\lfloor \frac{(q-1)n}{w} A_q(n-1,d,w-1) \right\rfloor.$$

c) *Conclude that, for any* $i \le w$

$$A_q(n,d,w) \le \left\lfloor \frac{(q-1)n}{w} \left\lfloor \frac{(q-1)(n-1)}{w-1} \left\lfloor \cdots \left\lfloor \frac{(q-1)(n-i+1)}{w-i+1} A_q(n-i,d,w-i) \right\rfloor \cdots \right\rfloor \right\rfloor \right\rfloor.$$

Theorem 47 (Unrestricted Johnson bound)**.** *Let* $d \le 2w$ *and* $e = \lceil d/2 \rceil$. *Then*

$$A_q(n,d,w) \le \left\lfloor \frac{(q-1)n}{w} \left\lfloor \frac{(q-1)(n-1)}{w-1} \left\lfloor \cdots \left\lfloor \frac{(q-1)(n-w+e)}{e} \right\rfloor \cdots \right\rfloor \right\rfloor \right\rfloor.$$

Problem 48. *Prove the theorem: apply the results of problem 46, with* $i = w-e+1$ *if* $d = 2e-1$, *and with* $i = w-e$ *if* $d = 2e$; *use problem 43 i).*