## 1. Weight Enumerators

Given a $[n,k,d]$ code $C$ over $\mathbb{F}_q$, let $A_j = |\{c \in C : w(c) = j\}|$. This set of parameters is the **weight distribution** of the code.
The polynomial $W_C(z) = \sum_{j=0}^{n} A_j z^j$ (i.e., the ordinary generating function associated with the sequence $(A_j)$) is the **weight enumerator** of $C$. The values $A_i$ carry important information about the code that can be applied to decoding problems.

**Proposition 1.** *Let $C$ be a $[n,k,d]$ code over $\mathbb{F}_q$. Then*

a) *$A_0 = 1$ and $A_j = 0$ for $0 < j < d$.*
b) *$\sum_j A_j = q^k$.*
c) *If $q = 2$ and $C$ contains the vector $11\cdots1$ ($v_i = 1$ for $1 \leq i \leq n$), then $A_j = A_{n-j}$.*

*Proof.* **HW**. □

**Exercise 2.** *Express the statements of the previous proposition as properties of the function $W_C(z)$.*

**Example 3.** *Let $C$ be the binary code with generator matrix*

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

*Then (**HW**) $W_C(z) = 1 + 2z^3 + z^4$.*

**Remark 4.** *In a linear code the number of codewords at distance i from a fixed codeword c does not depend on c (**HW**). In a nonlinear code this does not have to happen (a code with this property is called **distance-invariant**) and so the weight distribution does not characterize the distances between code words.*
*For a general $(n, M, d)$ code we define the **distance distribution** coefficients as*

$$d_i(C) = \frac{1}{M}(\text{ number of ordered pairs } u, v \text{ of codewords such that } \operatorname{dist}(u,v) = i).$$

### 1.1. MacWilliams equations.

The direct computation of the weight distribution of a code may be extremely difficult. One of the most useful tools to circumvent that problem is a set of equalities, the MacWilliams equations, that relate the weight distribution coefficients $A_j$ of $C$ with those of $C^\perp$, which we denote as $A_j^\perp$. However, in the process of deduction of the MacWilliams equalities, we use, for clarity, the notation $B_j$.

As $A_0 = 1$ and $\sum_{j=0}^{n} A_j = q^k$ for any linear $[n,k]$ code over $\mathbb{F}_q$, we have a first equation

$$\sum_{j=0}^{n} A_j = q^k B_0.$$

Let $L$ be a $q^k \times n$ matrix whose rows are the codewords of $C$ in some order. We count the zero entries of $L$ in two different ways: counting by rows we have that the number is $\sum_{j=0}^{n}(n-j)A_j$; on the other hand, we have that, for a fixed coordinate

$i$, either $col_i(L)$ is the zero vector, or it contains the same number of copies of each $x \in \mathbb{F}_q$: the projection

$$\phi_i : C \to \mathbb{F}_q, \qquad \phi_i(c) = c_i$$

is either the zero map or it is surjective and, if this is the case, the sets $\{c \in C : c_i = x\}$ are the cosets of the kernel of $\phi_i$ and so they all have the same cardinality $q^{k-1}$.
But the number of zero columns of $L$ is $\frac{B_1}{q-1}$, so the total number of zero entries is

$$\frac{q^k}{q-1}B_1 + \left(n - \frac{B_1}{q-1}\right) q^{k-1} = q^{k-1}(nB_0 + B_1).$$

These two counts give the second equation

$$\sum_{j=0}^{n}(n-j)A_j = q^{k-1}(nB_0 + B_1).$$

The strategy to find the remaining equalities is based on the same idea of counting in two ways $l$-tuples of zeros in the rows of $L$.
Let $N_l$ be the number of $l$-tuples of (not necessarily consecutive) zeros in the rows of $L$. A row of weight $j$ has $\binom{n-j}{l}$ $l$-tuples and so

$$N_l = \sum_{j=0}^{n} \binom{n-j}{l} A_j.$$

If, on the other hand, we fix a $l$-tuple $S \subset [n]$ of columns and consider the corresponding submatrix of $L$, we see that - denoting by $\bar{S}$ the complement $[n] \setminus S$ of $S$ - its distinct rows correspond to vectors of $C^{[\bar{S}]}$ (the puncturing of $C$ in $\bar{S}$); puncturing is a linear surjective map, so its kernel has $q^{k-k_S}$ where $k_S$ is the dimension of $C^{[\bar{S}]}$. So

$$N_l = \sum_{|S|=l} q^{k-k_S} = q^{k-l} \sum_{|S|=l} q^{l-k_S};$$

if we denote by $D_j(S)$ the weight coefficients of $\left(C^{[\bar{S}]}\right)^{\perp}$, which is a $[|S|, |S| - k_S]$ code, we may apply a previous equality to obtain

$$N_l = q^{k-l} \sum_{|S|=l} \sum_{j=0}^{l} D_j(S) = q^{k-l} \sum_{j=0}^{l} \sum_{|S|=l} D_j(S).$$

But $\left(C^{[\bar{S}]}\right)^{\perp} = \left(C^{\perp}\right)_{[\bar{S}]}$, where the right-hand side is the shortening of the dual of $C$ at the complement of $S$, and so a vector with weight $j$ in $\left(C^{[\bar{S}]}\right)^{\perp}$ is the puncturing of a $x \in C^{\perp}$ with weight $j$ and support contained in $S$.
This means that $\sum_{|S|=l} D_j(S)$ counts the number of elements of

$$T = \{(x, S) : x \in C^{\perp}; w(x) = j; \mathrm{supp}(x) \subset S; |S| = l\}.$$

Now, for each $x \in C^\perp$ with weight $j$, there are $\binom{n-j}{l-j}$ sets $S \subset [n]$ with $l$ elements containing $\operatorname{supp}(x)$; so

$$\sum_{|S|=l} B_j(S) = |T| = \binom{n-j}{l-j} B_j.$$

Putting everything together, we have
+

**Theorem 5** (MacWilliams Equalities). *The weight distribution coefficients of $C$ and $C^\perp$ satisfy the equalities*

$$\sum_{j=0}^{n-l} \binom{n-j}{l} A_j = q^{k-l} \sum_{j=0}^{l} \binom{n-j}{n-l} A_j^\perp \ \forall l \leq n.$$

As $\binom{m}{t} = 0$ if $t > m$, the equations may be writen in matrix form as

$$\left[\binom{n-j}{l}\right]_{0\leq l\leq n}^{0\leq j\leq n} (A_j) = D \left[\binom{n-j}{n-l}\right]_{0\leq l\leq n}^{0\leq j\leq n} (A_j^\perp)$$

where $D$ is the diagonal matrix with diagonal entries $q^{k-l}$, $0 \leq l \leq n$.

The MacWilliams equalities have several equivalent formulations. Some of them involve the **weight enumerator** $W_C(z)$. If we replace $z$ by $z/y$ and multiply by $y^n$ we obtain a two variable generating function $W_C(z, y) = \sum_j A_j z^j y^{n-j}$.

**Proposition 6.** *The following equation is equivalent to the MacWilliams equalities:*

$$W_{C^\perp}(z, y) = \frac{1}{q^k} W_C(y - z, y + (q - 1)z).$$

*Proof.* If we consider the variable $u = y - z$, the equality stated becomes

$$W_{C^\perp}(z, u + z) = \frac{1}{q^k} W_C(u, u + qz),$$

or

$$\sum_{i=}^{n} B_i z^i (u + z)^{n-i} = \frac{1}{q^k} \sum_{i=0}^{n} A_i u^i (u + qz)^{n-i}.$$

Applying Newton's binomial formula and changing the order of summation on both sides, the equality is easily seen to be equivalent to the MacWilliams equalities. The details are left as an exercise (**HW**). □

**Exercise 7.** *Consider the code* $[6, 3]$ $C$ *over* $\mathbb{F}_3$ *with generator matrix*

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 2 & 1 \\ 0 & 1 & 0 & 2 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

a) *Verify directly that $C$ and $C^\perp$ have both minimal distance 3 and that*

$$A_0 = A_0^\perp = 1, \qquad A_3 = A_3^\perp = 6.$$

b) *Use the MacWilliams equalities to deduce the remaining weight coefficients.*

**Exercise 8.** *Show that exchanging the roles of $C$ and $C^\perp$ in*

$$W_{C^\perp}(z,y) = \frac{1}{q^k} W_C(y-z, y+(q-1)z),$$

*and replacing $z$ with $y+u$ results in the following equivalent form of MacWilliams equalities:*

$$\sum_{j=t}^{n} \binom{j}{t} A_j = q^{k-t} \sum_{i=0}^{t} (-1)^i \binom{n-i}{n-t} (q-1)^{t-i} B_i \ \forall 0 \le t \le n.$$

**Exercise 9.** *Recall that a $q$-ary Hamming code $C$ is defined by a parity-check matrix $H$ whose columns are representatives of the different $1$-dimensional subspaces of $\mathbb{F}_q^m$. It is a $[\frac{q^m-1}{q-1}, \frac{q^m-1}{q-1} - m, 3]$-code.*

a) *Compute the weight coefficients and the weight enumerator of the simplex code dual of the Hamming code described above;*

b) *Compute the weight coefficients and the weight enumerator of the Hamming codes with $m=2$, for $q=5$ and $q=7$.*

***Hint for a):*** *the weight of a codeword of the simplex code is determined by the number of $1$-dimensional subspaces of $\mathbb{F}_q^m$ that are orthogonal to a given vector.*
***Hint for b):*** *Use Exercise 10.*

**Exercise 10.** *Show that, if $W_C(z)$ is the weight enumerator of a binary code $C$ then*

a) $W_{C_e}(z) = \frac{1}{2}(W_C(z) + W_C(-z))$ *where* $C_e = \{c \in C : w(c) \equiv 0 \mod 2\}$*;*

b) $W_{\hat{C}} = \frac{1}{2}((1+z)W_C(z) + (1-z)W_C(-z))$ *where $\hat{C}$ is the parity extension of $C$.*

**Exercise 11.** *Find all possible weight enumerators of binary self-dual $[8,4]$ codes.*

**Exercise 12.** *Show that the weight enumerator of the direct sum of two codes satisfies*

$$W_{C_1 \oplus C_2}(z) = W_{C_1}(z) W_{C_2}(z).$$

1.2. **Weight Enumeration and Generating Functions: an example.** The computation of the $A_j$ may be a hard problem. In special cases, the properties of the code alows for a more direct computation. We consider here the case of the binary Hamming codes. It provides a good example of application of ideas from Enumerative Combinatorics.

**Remark 13.** ***Warning:*** *This example involves the solution of a differential equation, a subject which is not a prerequisite of this course and that will be not used elsewhere.*

**Example 14.** *Let $C$ be the binary Hamming code with length $n = 2^t - 1$ and let $H$ denote a parity-check matrix. We start with the obvious observation, valid for any binary linear code, that the codewords with weight $j$ correspond to the sets of $j$ columns of $H$ with zero sum (**HW**).*

*We now take advantage of the fact that the columns of $H$ are all the nonzero vectors in $\mathbb{F}_2^t$. So, a set of $j$ columns with zero sum corresponds, non-uniquely, to a set of $j - 1$ columns (because we may always choose one last column to obtain the zero sum).*

*We may choose $j - 1$ columns in $\binom{n}{j-1}$ ways, and there are three possibilities:*

- i) *the sum of those columns is 0;*
- ii) *the sum of those columns is one of the chosen columns;*
- iii) *the sum of those columns is one of the remaining columns.*

**Exercise 15.** *Show that case i) occurs $A_{j-1}$ times, case ii) occurs $(n-(j-2))A_{j-2}$ times, and case iii) occurs $jA_j$ times.*

*So we have*

$$jA_j = \binom{n}{j-1} - A_{j-1} - (n - (j-2))A_{j-2}.$$

*Notice (**HW**) that the deduction is valid for $2 \leq j \leq n + 1$ (and even for $j = 1$, if we assume that the sum of an empty set is zero by definition), but that the equality remains trivially correct for $j > n + 1$.*

*We use now a standard technique of generating functions: we multiply the equality by $z^{j-1}$ and sum over $j$:*

$$\sum_j jA_j z^{j-1} = \sum_j \binom{n}{j-1} z^{j-1} - \sum_j A_{j-1} z^{j-1} - \sum_j (n - (j-2))A_{j-2} z^{j-1}.$$

*We may let $j$ vary over all positive integers as, in each of the sums, the summand is zero outside of a given interval:*

*The left-hand side is $W_C'(z)$, the derivative of the weight enumerator. For the first two sums on the right-hand side we have*

$$\sum_j \binom{n}{j-1} z^{j-1} = \sum_{j=1}^{n+1} \binom{n}{j-1} z^{j-1} = \sum_{l=0}^{n} \binom{n}{l} z^l = (1+z)^n,$$

*and*

$$\sum_j A_{j-1} z^{j-1} = \sum_{j=1}^{n+1} A_{j-1} z^{j-1} = \sum_{l}^{n} A_l z^l = W_C(z).$$

*The last sum needs a bit more work, along the same lines:*

$$\sum_j (n - (j-2))A_{j-2} z^{j-1} = nz \sum_{j=2}^{n+2} A_{j-2} z^{j-2} - z^2 \sum_{j=3}^{n+2} (j-2)A_{j-2} z^{j-3} =$$

$$= nz \sum_{l=0}^{n} A_l z^l - z^2 \sum_{l=1}^{n} lA_l z^{l-1} = nzW_C(z) - z^2 W_C'(z).$$

*We end up with the differential equation*

$$(1 - z^2)W_C'(z) = (1+z)^n - (1+nz)W_C(z),$$

*which happens to have, given the initial condition* $W_C(0) = 1$, *the unique solution*

$$W_C(z) = \frac{1}{n+1}(1+z)^n + \frac{n}{n+1}(1+z)^{(n-1)/2}(1-z)^{(n+1)/2}.$$

1.3. **Weight coefficients of MDS codes.** In general, the weight coefficients of a code are not determined by the basic parameters like length, size, distance and field over which it is defined. MDS codes are an exception:

**Theorem 16.** *If* $C$ *is a* $[n, k, d]$ *MDS code over* $\mathbb{F}_q$, *then*

$$A_i = \binom{n}{i} \sum_{j=0}^{i-d} (-1)^j \binom{i}{j} (q^{i+1-d-j} - 1),\ \forall d \leq i \leq n.$$

The proof consists on a clever application of ideas and techniques from enumerative combinatorics.

*Proof.* Given a $T \subset [n]$ with $|T| = t$, the shortening $C_{[T]}$ is a $[n-t, k-t, d]$ MDS code if $t < k$ (and the zero code otherwise). So $C(T)$ (the subcode $\{c \in C : c_i = 0\, \forall i \in T\}$) has size

$$|C(T)| = \begin{cases} q^{k-t} & \text{if } t < k \\ 1 & \text{if } t \geq k \end{cases}$$

and so, for each $0 \leq l \leq n$, we have

$$N_t = \sum_{T \subset [n], |T| = t} |C(T)| = \begin{cases} \binom{n}{t} q^{k-t} & \text{if } t < k \\ \binom{n}{t} & \text{if } t \geq k \end{cases}$$

$N_t$ counts the codewords with $w(c) \leq n - t$, each codeword being counted once for each $T$ such that $\operatorname{supp}(c) \subset [n] \setminus T$. So, if $w(c) = i$, $c$ is counted $\binom{n-i}{t}$ times and therefore

$$N_t = \sum_{i=0}^{n-t} A_i \binom{n-i}{t}.$$

We now want use these equations to recover the $A_i$ from the $N_t$. The following computation is an application of the Principle of Inclusion-Exclusion: Fixing $i$

$$\sum_{j=0}^{i} (-1)^j \binom{n-i+j}{j} N_{n-i+j} = \sum_{j=0}^{i} (-1)^j \binom{n-i+j}{j} \sum_{l=0}^{i-j} A_l \binom{n-l}{n-i+j} =$$

reversing the order of summation

$$= \sum_{l=0}^{i} A_l \sum_{j=0}^{i-l} (-1)^j \binom{n-l}{n-i+j} \binom{n-i+j}{j} = \sum_{l=0}^{i} A_l \sum_{j=0}^{i-l} (-1)^j \binom{n-l}{n-i} \binom{i-l}{j},$$

using a well known identity of binomial coefficients:

$$\binom{a}{b+c} \binom{b+c}{c} = \binom{a}{b} \binom{a-b}{c};$$

this can be verified by direct inspection of the explicit expressions for the binomial coefficients in terms of factorials, or, better still, by a counting argument.

We obtain

$$\sum_{l=0}^{i} A_l \binom{n-l}{n-i} \sum_{j=0}^{i-l} (-1)^j \binom{i-l}{j};$$

but the inner sum equals 0 if $i > l$ and 1 if $i = l$ and so we get

$$A_i = \sum_{j=0}^{i} (-1)^j \binom{n-i+j}{j} N_{n-i+j};$$

we use the expressions obtained before for $N_t$, separating the values of $j$ such that $n-i+j < k$ from the others:

$$A_i = \sum_{j=0}^{k-n+i-1} (-1)^j \binom{n-i+j}{j} \binom{n}{n-i+j} q^{k-(n-i+j)} + \sum_{j=k-n+i}^{i} (-1)^j \binom{n-i+j}{j} \binom{n}{n-i+j} =$$

using the same relation as above

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

using the equality $n-k+1 = d$

$$= \binom{n}{i} \left( \sum_{j=0}^{i-d} (-1)^j \binom{i}{j} q^{i+1-d-j} + \sum_{j=i-d+1}^{i} (-1)^j \binom{i}{j} \right) =$$

applying again the Binomial theorem to the second sum

$$= \binom{n}{i} \left( \sum_{j=0}^{i-d} (-1)^j \binom{i}{j} q^{i+1-d-j} - \sum_{j=0}^{i-d} (-1)^j \binom{i}{j} \right) = \binom{n}{i} \sum_{j=0}^{i-d} (-1)^j \binom{i}{j} \left( q^{i+1-d-j} - 1 \right).$$

□

Repetition codes are clearly MDS $[n, 1, n]$ codes. Their duals are also MDS with parameters $[n, n-1, 2]$. These are considered to be the trivial MDS codes. We notice that these codes exist for arbitrary $n$, independently of the field.
We will see, as a simple consequence of the previous theorem, that this is not the case for non-trivial MDS codes. In fact, if $C$ is a $[n, k, n-k+1]$ code over $\mathbb{F}_q$ with $1 < k$ (and so $d < n$), then

$$A_{d+1} = \binom{n}{d+1} [(q^2 - 1) - (d+1)(q-1)] = \binom{n}{d+1} (q-1)(q-d),$$

which implies that $n - k + 1 = d \leq q$.
Applying the same reasoning to $C^{\perp}$, which is a $[n, n-k, k+1]$ code, we have $k + 1 \leq q$. In conclusion,

**Proposition 17.** *If $C$ is a MDS $[n, k, n-k+1]$ code over $\mathbb{F}_q$ and $1 < k < n-1$, then*

$$k \leq q - 1, \qquad n \leq q + k - 1 \leq 2(q-1).$$

1.4. **Relation with probability of decoding error.** REcall that assuming the conditions that guarantee the equivalence of Minimal Distance Decoding and Maximal Likelihood Decoding,

i) The input probability distribution is uniform;
ii) The channel forward probabilities are

$$p(y_j|x_i) = \begin{cases} 1-\rho & \text{if } y_j = x_i \\ \\ \frac{\rho}{q-1} & \text{if } y_j \neq x_i \end{cases}$$

for some $0 \leq \rho < 1/2$,

we have

**Proposition 18.** *The probability of an error pattern to be undetected is*

$$p_{ed} = \sum_{i=1}^{n} A_i \left(\frac{\rho}{q-1}\right)^i (1-\rho)^{n-i}$$

*where $A_i$ denotes the number of codewords with weight $i$.*

*Proof.* **HW**. □

The result of this proposition can be rewritten as

$$p_{ed} = [1-\rho]^n (W_C(\delta) - 1)$$

where $\delta = \frac{\rho}{(q-1)(1-\rho)}$.

**Exercise 19.** *Consider the binary code $C$ with generator matrix*

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

*Determine the weight distribution of $C$ and, assuming $C$ is being used for transmission through the channel described above (for $q = 2$), compute the probability of detection error.*

We discuss now another situation relating the weight enumerator with probability of error, this time only for binary codes. Many details will be left as an exercise (**HW**).

Assume that the input probability distribution is uniform and that the channel forward probabilities are given by the matrix

$$\begin{bmatrix} 1-\rho & \rho \\ \tau & 1-\tau \end{bmatrix}$$

Suppose that codewords from a $[n, k, d]$ binary code are transmitted through this channel and decoded using Maximum Likelyhood decoding. Consider first that the zero codeword (which we denote as 0) is sent; if $y$ is received, it will be decoded into $c$ such that $p(y|c)$ is minimal; if $p(y|c) > p(y|0)$ the decoding procedure will not output 0 and we have a decoding error. So, if

$$Y_c = \{y \in \mathbb{F}_2^n : p(y|c) \geq p(y|0)\},$$

the probability of decoding error in this case satisfies

$$p_e(0) = \sum_{y \in \cup_c Y_c} p(y|0) \leq \sum_{c \in C \setminus \{0\}} Q_c$$

where

$$Q_c = \sum_{y \in Y_c} p(y|0).$$

The condition defining $Y_c$ implies then that $Q_c \leq \sum_{y \in Y_c} \sqrt{p(y|c)p(y|0)}$ and so also

$$Q_c \leq \sum_{y \in \mathbb{F}_2^n} \sqrt{p(y|c)p(y|0)} = \sum_{y \in \mathbb{F}_2^n} \prod_{i=1}^{n} \sqrt{p(y_i|c_i)p(y_i|0)};$$

notice that, separating the summands with $y_1 = 0$ from those with $y_1 = 1$,

$$\sum_{y \in \mathbb{F}_2^n} \prod_{i=1}^{n} \sqrt{p(y_i|c_i)p(y_i|0)} =$$

$$= (\sqrt{p(0|c_1)p(0|0)} + \sqrt{p(1|c_1)p(1|0)}) \sum_{y \in \mathbb{F}_2^{n-1}} \prod_{i=2}^{n} \sqrt{p(y_i|c_i)p(y_i|0)};$$

and repeating this (or using induction (**HW**) we get

$$Q_c \leq \prod_{i=1}^{n} \sum_{y \in \mathbb{F}_2} \sqrt{p(y_i|c_i)p(y_i|0)}.$$

denoting $\lambda = \sqrt{p(0|1)p(0|0)} + \sqrt{p(1|1)p(1|0)}$, we conclude finally (**HW**) that

$$Q_c \leq \lambda^{w(c)}$$

and so

$$p_e(0) \leq \sum_{c \in C \setminus \{0\}} \lambda^{w(c)} = \sum_{i=1}^{n} A_i \lambda^i = W_C(\lambda) - 1.$$

If the sent codeword is $d \neq 0$, the same reasoning leads to

$$p_e(d) \leq \sum_{c \in C \setminus \{d\}} \lambda^{dist(c,d)}$$

but the number of codewords at distance $i$ from $d$ is equal to the number of codewords with weight $i$ and so we have the same estimate

**Proposition 20.** *If a binary code is used in a Binary channel, the probability of error satisfies*

$$p_e(d) \leq W_C(\lambda) - 1,$$

*where* $\lambda = \lambda = \sqrt{p(0|1)p(0|0)} + \sqrt{p(1|1)p(1|0)}$.

**Exercise 21.** *If the channel is symmetric, this upper bound may be improved, in some cases:*

a) *Show that, if in the definition of the forward probabilities of the channel we have* $\tau = \rho < 1/2$ *(and so* $\lambda = 2\sqrt{\rho(1-\rho)}$*), then the condition defining* $Y_c$ *may be used to get the estimate*

$$Q_c \leq \begin{cases} \lambda^{w(c)} & \textit{if } w(c) \textit{ is even} \\ \lambda^{w(c)+1} & \textit{if } w(c) \textit{ is odd} \end{cases}$$

b) *Deduce the upper bound*

$$p_e(0) \leq \frac{1}{2}\left[(1+\lambda)W_C(\lambda) + (1-\lambda)W_C(-\lambda)\right] - 1.$$

***Hint for a):*** *Verify that, if* $y \in Y_c$ *and* $t$ *is the number of coordinates such that* $y_i = 0$ *and* $c_i = 1$*, then* $w(c) \geq 2t$*. Apply this, in the case of* $w(c)$ *odd, to strenght the inequality*

$$p(y|0) \leq \sqrt{p(y|c)p(y|0)}.$$