On the Probability of Incorrect Decoding for Linear Codes

Marco Frego(✉)

University of Trento, Trento, Italy
marco.frego@unitn.it

Abstract. In the literature of Error Correcting Codes (ECC) there are many probabilistic characterizations of different events that happen in the decoding process. Historically, the most considered parameters in the performance of a linear code are the Probability of Undetected Error and the probability of incorrect decoding, also known as Probability of Miscorrected Error. While there is agreement about the first, starting from the Seventies, basically four definitions of the Probability of Miscorrected Error are present in literature; aim of this work is to show that they are equivalent and, although different in the mathematical formulation, they yield exactly the same result. The gap of this missing proof is herein fulfilled and two examples with interesting properties are given.

Keywords: Linear code · Error probability · Miscorrected error · Error detection · Bounded distance decoding · Decoding error probabilities

1 Introduction

The performance of a (linear) error correcting code can be evaluated on the basis of many parameters. Depending on the application studied, one can focus on the distance of the code, its dimension, the information rate; or one can investigate what happens when the number of errors in transmission is greater than the correction capability of the code. Those events are studied in terms of error probabilities. In the decoding process, the events of major interest have an associated probability, in particular, the Probability of Correct Decoding ($\mathbb{P}_{\mathrm{CD}}$), the Probability of Undetected Error ($\mathbb{P}_{\mathrm{UE}}$) and the Probability of Miscorrected Error ($\mathbb{P}_{\mathrm{ME}}$), [15]. The presence of an undetected error is especially important when related to safety, e.g. when the codewords represent a feedback for danger. A miscorrected error can have heavy consequences when the wrong information can corrupt a whole set of data, that is, the cost of incorrect decoding is high, for example in data storage applications or in the 3D reconstruction of a human body [1].

There are four formulations for the $\mathbb{P}_{\mathrm{ME}}$ and they have been derived by different authors from different points of view, also the mathematical expression is not the same but after a computer implementation and evaluation of the four formulas, it becomes clear that they give the same result. Therefore it is interesting to prove their equivalence, which is missing in literature.

M. O'Neill (Ed.): IMACC 2017, LNCS 10655, pp. 103–115, 2017.
https://doi.org/10.1007/978-3-319-71045-7_5

The work has this structure: Sect. 2 gives a short review of the names, conventions and standard use of symbols for ECC that will be useful for Sect. 3, where the four formulations of $\mathbb{P}_{\text{ME}}$ are stated and the equivalence theorem is proved. Section 4 presents a comparison of the results of bruteforce decoding (maximum likelihood) with the theoretical results of the probability of miscorrected error. Section 5 contains comments and conclusions on those four different formulas proposed in literature.

2 Background and Framework

Let $\mathcal{C}$ be an $[n, k, d]$ linear code over $\mathbb{F}_q$ with weight distribution $A_0, A_1, \ldots, A_n$ and let the symbol error probability on a $q-$ary alphabet be p. The probability that a symbol is correctly transmitted over the channel is then $1 - p$. Assume that if an error does occur, then each of the $q - 1$ symbols aside from the correct symbol is equally likely to be received, with probability $\frac{p}{q-1}$ each. This hypothetical channel is called the $q-$ary symmetric channel or $q - \text{SC}$ for short, [4]. This is a standard framework in ECC.

Let τ be the number of errors that occurred in transmission. If $\tau = 0$ the decoder does not detect any error and does not decode the received vector, as it is in the code already. If $1 \leq \tau \leq t$, where $t := \lfloor \frac{d-1}{2} \rfloor$, the decoder detects the error and corrects it to the unique codeword at distance less than t from the received vector. However, if $\tau > t$ three models of decoder must be considered: the ideal bounded distance decoder, the maximum likelihood decoder and other types (e.g. Berlekamp-Massey, etc.). If more than t errors occur, two situations can happen: (a) there is a unique codeword at distance at most t from the received vector; (b) there is no codeword at a distance lower than $t + 1$ from the received vector. In case (a), every decoder will clearly correct the vector to that unique codeword, and the correction will be wrong, see Fig. 1. In case (b), the decoders exhibit different behaviours: the ideal bounded distance decoder will not attempt to correct the vector and will raise a flag of decoding failure; the maximum likelihood decoder will correct the vector to its closest codeword (which may not be unique); for other decoders the behaviour is not specified, see Figure 2.

Remark 1. As a remark, notice that the algorithm of Berlekamp-Massey can be approximated with an ideal decoder. This algorithm is based on the error locator polynomial, which has the properties that its roots give the locations of the errors occurred in transmission (for instance [3] for a Gröbner Basis derivation). For a number of errors $\tau \leq t$ the roots of the locator polynomial are valid positions and the correction is unambiguous. If there are more than t errors, the following cases can happen: 1. there exists a codeword at distance lower than t from the received vector and this produces a wrong correction; 2a. there does not exist any codeword at distance lower than $t + 1$ from the received vector and the decoder corrects wrong, 2b. as in 2a but the decoder corrects to the sent codeword, 2c. there does not exist any codeword at distance lower than $t + 1$

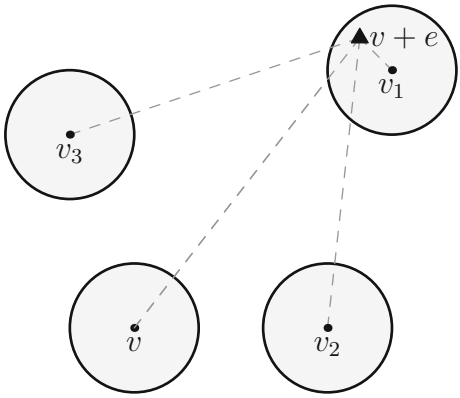

Fig. 1. Suppose to send v and receive $v + e$, i.e. the triangle inside the decoding sphere of v_1, in this case every decoder will correct $v + e$ to v_1 thus making a correction error.

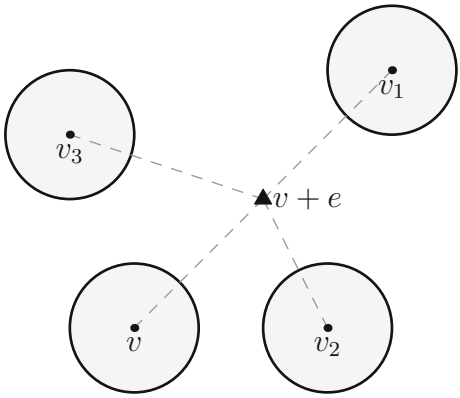

Fig. 2. Suppose to send v and receive $v+e$, i.e. the triangle outside any decoding sphere (in gray around each codeword). In this case the ideal decoder will raise a message of decoding failure, whereas the maximum likelihood decoder will decode to the closest codeword around $v + e$, that is v_2 in that picture.

from the received vector, but not all the roots of the locator polynomial are valid positions, the decoder sends a message of decoding failure. The case 2b cannot happen in practice because in this instance the locator polynomial will have a degree higher than t, but in an implementation, the decoding process will be stopped after degree t.

After these considerations about the decoders, we are interested in the probability of the miscorrected error for bounded distance decoders. It is important to notice that this decoding scheme is incomplete because not all possible received vectors will have a distance less than t from a codeword, that is, inside a decoding sphere, [12]. An example where the sent codeword is outside of any decoding

sphere is presented in Section 4, see also [10] for details about the decoding spheres. Consider the reliability of a bounded distance decoder. A codeword c sent over the channel is correctly decoded at the receiving end by the decoder if the decoder receives any vector in the sphere of radius $t = \lfloor \frac{d-1}{2} \rfloor$ around c, yielding a lower bound on the probability that a transmitted codeword is correctly decoded.

There are several different ways to characterize the error detecting and correcting capabilities of codes at the output of the channel decoder. Those are widely accepted definitions and they can be found in many references e.g. in [2,5,7,11,14].

$\mathbb{P}_{\mathrm{CD}}(p)$ is the *probability of correct decoding*, which is the probability that a codeword c sent over the channel is correctly decoded at the receiving end by the decoder, and can be computed by:

$$\mathbb{P}_{\mathrm{CD}}(p) = \sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i}.$$

Note that this probability is independent of the size of the alphabet. $\mathbb{P}_{\mathrm{UE}}(p)$ is the *probability of undetected error*, the probability that errors occurring in a codeword are not detected. An error vector moves the transmitted codeword into another codeword, and this probability is therefore

$$\mathbb{P}_{\mathrm{UE}}(p) = \sum_{i=d}^{n} A_i \left(\frac{p}{q-1} \right)^i (1-p)^{n-i}.$$

$\mathbb{P}_{\mathrm{E}}(w)$ is the *probability of miscorrected error conditioned to an error of weight* w. This is the probability that the codeword at the output of the decoder is not the same as the codeword produced by the encoder, with the condition that an error of weight w occurred. $\mathbb{P}_{\mathrm{ME}}(p)$ is the *probability of miscorrected error*. This is the probability that the decoder outputs a wrong codeword. It depends only on the code (it is important to note that knowledge of the weight distribution is required) and on the channel.

Whereas for the probabilities of correct decoding and undetected error there is agreement in the definition among all authors, the situation is very different for the $\mathbb{P}_{\mathrm{ME}}$. In the literature there are four definitions of $\mathbb{P}_{\mathrm{ME}}$, only one of them (proposed by [5]) involves the definition of $\mathbb{P}_{\mathrm{E}}(w)$, the others directly assume the presence of the $q-$ary symmetric channel. The study of the $\mathbb{P}_{\mathrm{ME}}$ in terms of the $\mathbb{P}_{\mathrm{E}}(w)$ brings more insight in what happens when the number of errors increases, therefore it is herein briefly summarized.

In order to proceed, define the quantity $N(\ell, w; s)$ as the number of vectors of weight w that are at distance s from a fixed codeword of weight ℓ. If w is not such that $\ell - s \leq w \leq \ell + s$, then $N(\ell, w; s) = 0$. $N(\ell, w; s)$ is independent of the given codeword of weight ℓ and is hence well defined ([5]). For $s \leq t$, spheres of radius s about codewords are disjoint and hence the number of vectors of weight w at distance exactly s from a codeword of weight ℓ is $A_\ell \cdot N(\ell, w; s)$.

Now received vectors which will be improperly decoded are those which lie within a sphere of radius t about some codeword other than that which was sent. Call C_w the number of these vectors, clearly

$$C_w = \sum_{\ell=0}^{n} A_\ell \sum_{s=0}^{t} N(\ell, w; s) \quad \text{for } t+1 \leq w \leq n.$$

This leads easily to the next lemma.

Lemma 1. *The probability $\mathbb{P}_{\mathrm{E}}(w)$ is the probability of miscorrected error conditioned to an error of weight w and is characterized by*

$$\mathbb{P}_{\mathrm{E}}(w) = \frac{C_w}{(q-1)^w \binom{n}{w}}.$$

Proof. $\mathbb{P}_{\mathrm{E}}(w)$ is given by the ratio of the *decodable* vectors of weight w (i.e. C_w) by all possible vectors of weight w, which are $(q-1)^w \binom{n}{w}$.

The following lemma finds out the number $N(\ell, w; s)$.

Lemma 2. *The number $N(\ell, w; s)$ of vectors of weight w that are at distance s from a fixed codeword of weight ℓ is zero if w is not such that $\ell - s \leq w \leq \ell + s$, otherwise is*

$$N(\ell, w; s) = \sum_{r=r_1}^{r_2} \binom{\ell}{\ell - s + r} \binom{s - r}{w - \ell + s - 2r} \binom{n - \ell}{r} (q-2)^{w-\ell+s-2r} (q-1)^r,$$

where $r_1 := \max\{0, w - \ell\}$ and $r_2 := \lfloor \frac{w-\ell+s}{2} \rfloor$. Note that $\lfloor x \rfloor$ is the larger integer less than or equal to x and that $\binom{x}{y}$ is zero if $y \notin \mathbb{N}$.

Proof. See [5]. □

Corollary 1. *In the case of binary linear codes $q = 2$ and the previous lemma simplifies to*

$$N(\ell, w; s) = \begin{cases} \binom{n-\ell}{\frac{s+w-\ell}{2}} \binom{\ell}{\frac{s-w+\ell}{2}} & \text{if } |w - \ell| \leq s \\ 0 & \text{if } |w - \ell| > s. \end{cases}$$

Once the weight distribution of $\mathcal{C}$ and $\mathbb{P}_{\mathrm{E}}(w)$ are known, the formula for the probability that the decoder outputs a wrong codeword is given by the next theorem.

Theorem 1. *The probability of miscorrected error $\mathbb{P}_{\mathrm{ME}}(p)$ depends only on the code $\mathcal{C}$ and on the channel ϕ, and is*

$$\mathbb{P}_{\mathrm{ME}}(p) := \mathbb{P}_{\mathrm{ME}}(\mathcal{C}, \phi) = \sum_{w=t+1}^{n} \mathbb{P}_{\mathrm{E}}(w) \phi(w), \tag{1}$$

where $\phi(w)$ is the probability of w errors in transmission. In the case of the $q-$ary symmetric channel $\phi(w)$ has the classic form

$$\phi(w) = \binom{n}{w}(q-1)^w \left(\frac{p}{q-1}\right)^w (1-p)^{n-w}.$$

Corollary 2. *In the $q-$ary symmetric channel, the probability of miscorrected error (1) simplifies to*

$$\mathbb{P}_{\mathrm{ME}}(\mathcal{C}, q-\mathrm{SC}) = \sum_{w=t+1}^{n} C_w \left(\frac{p}{q-1}\right)^w (1-p)^{n-w}.$$

It may be difficult to compute exactly this probability because the weight distribution of a linear code (or even just the minimum distance) is in general not known, [9]. In these cases the weight distribution can be approximated by suitable estimates and (1) becomes a bound.

3 Unified Probability of Miscorrected Error

This section collects the four formulations of the $\mathbb{P}_{\mathrm{ME}}$ found from different authors in literature. They are reported in four lemmas identified with the letters A, B, C and D. The corresponding expression for the $\mathbb{P}_{\mathrm{ME}}$ has a superscript with the matching letter. In the previous section the approach of [5] was presented, which turns out to be the most followed (Lemma 5), maybe because it was the first proposed. In [2] there is a historical description and bibliography of the papers and previous results that yield to [5]. With the aim of keeping the paper contained, the derivation of the four characterizations is skipped, but can be easily retrieved in each of the cited references.

Lemma 3 ([13]).

$$\mathbb{P}^A_{\mathrm{ME}}(p) = \sum_{\ell=2t+1}^{n} A_\ell \sum_{s=0}^{t}\sum_{r=0}^{t-s} \binom{n-\ell}{s}\binom{\ell}{r} \cdot (q-1)^{r-\ell}\left(1-\frac{p}{q-1}\right)^r (1-p)^{n-\ell-s} p^{\ell+s-r}.$$

Lemma 4 ([8,12,14]).

$$\mathbb{P}^B_{\mathrm{ME}}(p) = \sum_{\ell=2t+1}^{n} A_\ell \sum_{s=0}^{t}\sum_{r=0}^{s} \binom{n-\ell}{r}\binom{\ell}{s-r} \cdot \left(\frac{p}{q-1}\right)^{\ell-s+r}\left(1-\frac{p}{q-1}\right)^{s-r} (1-p)^{n-\ell-r} p^r.$$

Lemma 5 ([2,5,6]). *For r_1 and r_2 as defined in Lemma 2,*

$$\mathbb{P}^{C}_{\mathrm{ME}}(p) = \sum_{\ell=0}^{n} A_\ell \sum_{s=0}^{t} \sum_{w=t+1}^{n} \sum_{r=r_1}^{r_2} \binom{n-\ell}{r} \cdot \binom{\ell}{\ell-s+r} \binom{s-r}{w-\ell+s-2r} \left(\frac{p}{q-1}\right)^{w} (1-p)^{n-w} \cdot (q-2)^{w-\ell+s-2r} (q-1)^{r}.$$

Lemma 6 ([11]).

$$\mathbb{P}^{D}_{\mathrm{ME}}(p) = \sum_{w=t+1}^{n} \left(\frac{p}{q-1}\right)^{w} (1-p)^{n-w} \sum_{\ell=\max(w-t,d)}^{\min(w+t,n)} A_\ell \sum_{s=|l-w|}^{t} \sum_{r=0}^{s} \binom{\ell}{r} \binom{n-\ell}{r+w-\ell} \binom{\ell-r}{s+\ell-w-2r} \cdot (q-2)^{s+\ell-w-2r} (q-1)^{r+w-\ell}.$$

A final technical lemma is needed in order to prove the main theorem of this section.

Lemma 7. *The following identity holds:*

$$\sum_{j=0}^{s-r} \binom{s-r}{j} (q-2)^{j} (1-p)^{s-r-j} (q-1)^{r-s} = \sum_{j=0}^{s-r} \binom{s-r}{j} \left(\frac{p}{q-1}\right)^{j} (q-2)^{j} (1-p)^{s-r-j},$$

which, in particular, is equal to $\left(\frac{q-p-1}{q-1}\right)^{s-r}$.

Proof. Follows easily with Newton's Binomial Theorem. □

Theorem 2 (Unified Error Probability). *The four Lemmas 3, 4, 5 and 6 are equivalent.*

Proof. The proof is divided in three parts: Lemma 3 $\iff$ Lemma 4, then Lemma 5 $\iff$ Lemma 6 and finally Lemma 4 $\iff$ Lemma 5. First consider the equivalence of Lemma 3 and Lemma 4. The outer sum over ℓ is the same in (3) and (4), hence look at the inner part only. Starting from the binomial part of equation (4), the first observation is that $s \leq t$ and $r \leq s$, otherwise the binomial $\binom{\ell}{s-r}$ would become zero because of $s - r < 0$. It is possible to rewrite (4) as

$$\sum_{\ell=2t+1}^{n} A_\ell \sum_{s=0}^{t} \sum_{r=0}^{t} \binom{n-\ell}{r} \binom{\ell}{s-r} \left(\frac{p}{q-1}\right)^{\ell-s+r} \left(1-\frac{p}{q-1}\right)^{s-r} (1-p)^{n-\ell-r} p^{r}$$

and the swap r with s yields

$$\sum_{\ell=2t+1}^{n} A_\ell \sum_{s=0}^{t}\sum_{r=0}^{t} \binom{n-\ell}{s}\binom{\ell}{r-s}\left(\frac{p}{q-1}\right)^{\ell-r+s}\left(1-\frac{p}{q-1}\right)^{r-s}(1-p)^{n-\ell-s}p^s$$

Observing that the terms of the sum for the index $r = 0, 1, \ldots, s-1$ are zero, the previous expression is simplified (with the index substitution $k = r - s$, $r = k + s$) in

$$\sum_{\ell=2t+1}^{n} A_\ell \sum_{s=0}^{t}\sum_{k=0}^{t-s} \binom{n-\ell}{s}\binom{\ell}{k}\cdot(q-1)^{k-\ell}\left(1-\frac{p}{q-1}\right)^{k}(1-p)^{n-\ell-s}p^{\ell+s-k}.$$

After relabelling k with r, the result is exactly the same as $\mathbb{P}^A_{\mathrm{ME}}(p)$ given in (3). Thus Lemma B is equivalent to Lemma A.

Equivalence of Lemmas 5 and 6. Consider now Lemma 5, a preventive simplification shows that the index of the outer sum over ℓ can be made start from $d = 2t+1$ because for $\ell = 0$ the binomial term $\binom{\ell}{\ell-s+r} = 0$. Then for $\ell = 1, \ldots, 2t$ the weights A_ℓ of the code are all zero. The same binomial can be substituted by symmetry with $\binom{\ell}{s-r}$. With similar reasoning on the binomials, it is possible to make the summation over r run from $r_1 = w-l$ or 0 to $r_2 = w-l+s$. In fact, e.g. for r_2, the binomial $\binom{s-r}{(w-l+s)-2r}$ will have a negative argument and thus is zero. Similarly, when r_1 is negative the first binomial has a negative argument, and for $0 \le r_1 < |w-l|$ the last binomial is zero. Hence the bounds r_1 and r_2 by [5] are very accurate and reduce the effort of computation over dummy indexes. Rewrite Lemma 5 as

$$\begin{aligned}\mathbb{P}^C_{\mathrm{ME}}(p) = &\sum_{\ell=2t+1}^{n} A_\ell \sum_{s=0}^{t}\sum_{w=t+1}^{n}\sum_{r=w-l}^{w-l+s} \binom{n-\ell}{r}\binom{\ell}{s-r}\binom{s-r}{w-\ell+s-2r}\\ &\cdot\left(\frac{p}{q-1}\right)^{w}(1-p)^{n-w}\cdot(q-2)^{w-\ell+s-2r}(q-1)^{r}. \qquad (2)\end{aligned}$$

In the formula (6) of Lemma 6, notice that $r, s \le t$ so that $r + s < 2t + 1 = d$. The sum over ℓ can run just over $\ell = d, \ldots, n$, because if $\ell - w > t$ the binomial $\binom{n-\ell}{r+w-\ell} = \binom{n-l}{r-(l-w)}$ will have a negative argument and is therefore zero, when $\ell - w < -t$, the third binomial has a negative argument. Thus it is possible to swap the sum over ℓ with the sum over w and obtain,

$$\begin{aligned}\mathbb{P}^D_{\mathrm{ME}}(p) = &\sum_{\ell=2t+1}^{n} A_\ell \sum_{w=t+1}^{n}\sum_{s=|l-w|}^{t}\sum_{r=0}^{s} \binom{\ell}{r}\binom{n-\ell}{r+w-\ell}\binom{\ell-r}{s+\ell-w-2r}\\ &\cdot\left(\frac{p}{q-1}\right)^{w}(1-p)^{n-w}\cdot(q-2)^{s+\ell-w-2r}(q-1)^{r+w-\ell}.\end{aligned}$$

Now with the change of variable $r \to r + w - \ell$ the new sum over r runs from $w - \ell$ to $s + w - l$, and the first binomial becomes, by symmetry, $\binom{\ell}{w-\ell}$. Observe then that the index s runs from t to zero, therefore it is possible to reorder the sum for $s = 0, \ldots, t$. Those simplifications lead to

$$\mathbb{P}^D_{\mathrm{ME}}(p) = \sum_{\ell=2t+1}^{n} A_\ell \sum_{w=t+1}^{n} \sum_{s=0}^{t} \sum_{r=w-\ell}^{s+w-\ell} \binom{\ell}{w-r}\binom{n-\ell}{r}\binom{w-r}{s+w-\ell-2r} \left(\frac{p}{q-1}\right)^w (1-p)^{n-w} \cdot (q-2)^r (q-1)^{s+w-\ell-2r},$$

which resembles equation (2) apart from the role of w in the three binomials. After a sharp look, it is possible to substitute the missing s with the w without changing the result, because of a combined simplification of the binomials, in particular:

$$\binom{n-\ell}{r}\binom{\ell}{w-r}\binom{w-r}{s+w-\ell-2r} = \binom{n-\ell}{r}\binom{\ell}{s-r}\binom{s-r}{w-\ell+s-2r},$$

which can be easily verified expanding with factorials. Therefore $\mathbb{P}^C_{\mathrm{ME}}(p) = \mathbb{P}^D_{\mathrm{ME}}(p)$.

The last part of the proof is that Lemma 4 is equivalent to Lemma 5: in Lemma 4 consider the quantity $1 - p/(q-1)$, it can be recast into $[(q-2) + (1-p)]/(q-1)$. Therefore, with Newton's Binomial Theorem, $[1 - p/(q-1)]^{s-r}$ becomes

$$\frac{1}{(q-1)^{s-r}} \sum_{j=0}^{s-r} \binom{s-r}{j} (q-2)^j (1-p)^{s-r-j}.$$

Hence, Lemma 4 can be expanded as,

$$\mathbb{P}^B_{\mathrm{ME}}(p) = \sum_{\ell=2t+1}^{n} A_\ell \sum_{s=0}^{t} \sum_{r=0}^{s} \sum_{j=0}^{s-r} \binom{n-\ell}{r}\binom{\ell}{s-r}\binom{s-r}{j} \cdot \left(\frac{p}{q-1}\right)^{\ell-s+r} (q-1)^{r-s} (q-2)^j (1-p)^{n-\ell-2r+s-j} p^r,$$

where, after collecting terms,

$$\mathbb{P}^B_{\mathrm{ME}}(p) = \sum_{\ell=2t+1}^{n} A_\ell \sum_{s=0}^{t} \sum_{r=0}^{s} \binom{n-\ell}{r}\binom{\ell}{s-r} \cdot \left(\frac{p}{q-1}\right)^{\ell-s+2r} (q-1)^r (1-p)^{n-\ell-r} \cdot \sum_{j=0}^{s-r} \binom{s-r}{j} (q-1)^{r-s-j} (q-2)^j (1-p)^{s-r-j}.$$

It is now possible to make use of Lemma 7 and substitute the last sum over j as follows:

$$\mathbb{P}^{B}_{\mathrm{ME}}(p) = \sum_{\ell=2t+1}^{n} A_\ell \sum_{s=0}^{t}\sum_{r=0}^{s}\sum_{j=0}^{s-r} \binom{n-\ell}{r}\binom{\ell}{s-r}\binom{s-r}{j} \cdot \left(\frac{p}{q-1}\right)^{j+\ell-s+2r} (q-1)^r (q-2)^j (1-p)^{n-(j+\ell-s+2r)}.$$

The substitution $w = j + \ell - s + 2r$ yields something that is almost equal to the modified version of Lemma 5 in equation (2):

$$\sum_{\ell=d}^{n} A_\ell \sum_{s=0}^{t}\sum_{r=0}^{s}\sum_{w=\ell-s+2r}^{\ell+r} \binom{n-\ell}{r}\binom{\ell}{s-r}\binom{s-r}{w-\ell+s-2r} \cdot \left(\frac{p}{q-1}\right)^{w} (q-1)^r (q-2)^{w-\ell+s-2r} (1-p)^{n-w}.$$

The differences with (2) are the order of the inner sums. To exchange the sum over r with the sum over w, the new indexes must be $w = \ell - s, \ldots, \ell + s$ and $r = w - \ell, \ldots, w - \ell + s$, where the upper limit of r was simplified using the same consideration on the third binomial discussed above for r_2. With similar considerations it is possible to extend the range of w to $w = t+1, \ldots, n$, because for values smaller than $\ell - s$ the first binomial will have a negative r and for values greater than $\ell + s$ the other binomials will have negative argument. The result is exactly $\mathbb{P}^{C}_{\mathrm{ME}}(p)$ and the proof is complete. □

4 An Application with Numerical Results

$\mathbb{P}_{\mathrm{D}}(p)$ is the *probability of detected codeword error*, the probability that one or more errors occurring in a codeword are detected. $\mathbb{P}_{\mathrm{F}}(p)$ is the *probability of decoder failure*, which is the probability that the decoder is unable to decode the received vector (and is able to determine that it cannot decode). The following check is performed: comparison between the theoretical $\mathbb{P}_{\mathrm{E}}(w)$ and the "real" one, obtained by bruteforce decoding, this last identified as $\mathbb{P}^{\mathrm{r}}_{\mathrm{E}}(w)$. Suppose to send the zero codeword, if an arbitrary error occurs, it is possible to receive every possible vector of $(\mathbb{F}_q)^n$. After the correction, five cases can happen:

1. the received vector lies in the correct decoding sphere and is decoded to the sent word;
2. the received vector lies in a wrong decoding sphere and is decoded to a wrong codeword;
3. the vector is outside of any decoding sphere but is close to only one codeword and is decoded to the sent word;
4. the vector is outside of any decoding sphere but is close to only one codeword and is decoded to a wrong codeword;

5. the vector is outside of any decoding sphere and there are more codewords at the same distance, so a decoding failure happens.

In the next examples all decoded vectors (according to the weight w of the error) are divided in three sets: the set D_w of the vectors correctly decoded (cases 1 and 3), the set S_w of the miscorrected vectors (cases 2 and 4), and the set of the failures F_w (case 5). The number C_w gives the number of elements of case 2, hence they are expected to be $|S_w| \geq C_w$. Furthermore $|S_0|, \ldots, |S_t|$ should be all zero. The next two toy examples show a case on $\mathbb{F}_2$ where $|S_w| = C_w$ and a case on $\mathbb{F}_3$ where $|S_w| > C_w$.

4.1 Example over $\mathbb{F}_2$

Let C be the linear code $[5, 2, 3]$ over $\mathbb{F}_2$ with generator matrix

$$G = \begin{pmatrix} 1\,0\,1\,0\,1 \\ 0\,1\,0\,1\,1 \end{pmatrix}.$$

In this example there is no difference between the theorical formula and the bruteforce, see Table 1.

Table 1. Results for the linear code $[5, 2, 3]$ over $\mathbb{F}_2$. A_w is the weight distribution, $|D_w|$ is the number of the vectors correctly decoded, $|F_w|$ the number of failures, $|S_w|$ the number of miscorrected vectors, $|C_w|$ the number of vectors in the wrong decoding sphere.

w	A_w	$\lvert D_w\rvert$	$\lvert F_w\rvert$	$\lvert S_w\rvert$	C_w	$\mathbb{P}_{\mathrm{E}}^{\mathrm{r}}(w)$	$\mathbb{P}_{\mathrm{E}}(w)$
0	1	1	0	0	(1)	0	0
1	0	5	0	0	(5)	0	0
2	0	0	4	6	6	3/5	3/5
3	2	0	4	6	6	3/5	3/5
4	1	0	0	5	5	1	1
5	0	0	0	1	1	1	1

4.2 Example over $\mathbb{F}_3$

Let C be the linear code $[5, 2, 3]$ over $\mathbb{F}_3$ with generator matrix

$$G = \begin{pmatrix} 1\,0\,1\,2\,0 \\ 0\,1\,0\,1\,1 \end{pmatrix}$$

In this example there are some vectors outside the decoding spheres, the results are collected in Table 2. Notice that $|S_w| > C_w$ and so $\mathbb{P}_{\mathrm{E}}^{\mathrm{r}}(w) \geq \mathbb{P}_{\mathrm{E}}(w)$.

Table 2. Results for the linear code $[5, 2, 3]$ over $\mathbb{F}_3$. A_w is the weight distribution, $|D_w|$ is the number of the vectors correctly decoded, $|F_w|$ the number of failures, $|S_w|$ the number of miscorrected vectors, $|C_w|$ the number of vectors in the wrong decoding sphere.

w	A_w	$\lvert D_w\rvert$	$\lvert F_w\rvert$	$\lvert S_w\rvert$	C_w	$\mathbb{P}_{\mathrm{E}}^{\mathrm{r}}(w)$	$\mathbb{P}_{\mathrm{E}}(w)$
0	1	1	0	0	(1)	0	0
1	0	10	0	0	(10)	0	0
2	0	8	20	12	12	3/10	3/10
3	4	0	16	64	24	4/5	3/10
4	2	0	28	52	36	13/20	9/20
5	2	0	8	24	16	3/4	1/2

5 Comments and Conclusions

In the literature of ECC there are at least four different formulations of the probability of miscorrected error. They have been presented in Lemmas 3, 4, 5 and 6, with some comments for Lemma 5, probably the most known. It has been proved that they are equivalent, hence it is useful to point out what is the most practical formula in terms of complexity. The complexity of Lemmas 3 and 4 is the same, the number of iterations of the sums required to evaluate the $\mathbb{P}_{\mathrm{ME}}(p)$ is $\gamma = \frac{1}{2}(n-2t)(t+2)(t+1) \leq n^3$, whereas for Lemmas 5 and 6 a rough estimate is $\gamma(n-t) \leq n^4$, which is one factor greater. Nevertheless, formulation of $\mathbb{P}_{\mathrm{ME}}^{C}(p)$ gives information on the $\mathbb{P}_{\mathrm{E}}(w)$ which can be useful in some applications, where the number of errors beyond t has importance.

References

1. Biasi, N., Setti, F., Del Bue, A., Tavernini, M., Lunardelli, M., Fornaser, A., Da Lio, M., De Cecco, M.: Garment-based motion capture (gamocap): high-density capture of human shape in motion. Mach. Vis. Appl. **26**(7–8), 955–973 (2015)
2. Blahut, R.E.: Theory and Practice of Error Control Codes. Addison-Wesley Pub. Co., Massachusetts (1983)
3. Caruso, F., Orsini, E., Sala, M., Tinnirello, C.: On the shape of the general error locator polynomial for cyclic codes. IEEE Trans. Inf. Theor. **63**(6), 3641–3657 (2017)
4. Faldum, A., Lafuente, J., Ochoa, G., Willems, W.: Error probabilities for bounded distance decoding. Des. Codes Crypt. **40**(2), 237–252 (2006)
5. Huntoon, Z., Michelson, A.: On the computation of the probability of post-decoding error events for block codes (corresp.). IEEE Trans. Inf. Theor. **23**(3), 399–403 (1977)
6. Kim, M.G., Lee, J.H.: Decoder error probability of binary linear block codes and its application to binary primitive bch codes. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **E79–A**(4), 592–599 (1996)

7. McWilliams, F.J., Sloane, N.J.A.: The Theory of Error-correcting Codes. North-Holland, Amsterdam (1977)
8. Moon, T.K.: Error Correction Coding: Mathematical Methods and Algorithms. Wiley-Interscience, Hoboken (2005)
9. Piva, M., Sala, M.: A new bound for cyclic codes beating the roos bound. In: Muntean, T., Poulakis, D., Rolland, R. (eds.) CAI 2013. LNCS, vol. 8080, pp. 101–112. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40663-8_11
10. Roman, S.: Introduction to Coding and Information Theory. Undergraduate Texts in Mathematics. Springer, New York (1997)
11. Torrieri, D.J.: Principles of Spread-Spectrum Communication Systems. Springer, Cham (2005)
12. Vanstone, S.A., van Oorschot, P.C.: An Introduction to Error Correcting Codes with Applications. Kluwer International Series in Engineering and Computer Science: Communications and Information Theory. Springer, New York (1989)
13. Wicker, S.B.: Reed-solomon error control coding for rayleigh fading channels with feedback. IEEE Trans. Veh. Technol. **41**(2), 124–133 (1992)
14. Wicker, S.B.: Error Control Systems for Digital Communication and Storage. Prentice Hall, New Jersey (1995)
15. Xia, S.-T., Fu, F.-W.: Undetected error probability of q-ary constant weight codes. Des. Codes Crypt. **48**(2), 125–140 (2008)