On the Decoder Error Probability for Reed-Solomon Codes

R. J. McEliece
California Institute of Technology

L. Swanson
Communications Systems Research Section

In this article we derive upper bounds on the decoder error probability for Reed-Solomon codes. By definition, "decoder error" occurs when the decoder finds a codeword other than the transmitted codeword, this is in contrast to "decoder failure," which occurs when the decoder fails to find any codeword at all. Our results imply, for example, that for a t *error-correcting Reed-Solomon code of length* q – *1 over* GF(q), *if more than* t *errors occur, the probability of decoder error is less than* $1/t!$. *In particular, for the Voyager Reed-Solomon code, the probability of decoder error given a word error is smaller than* 3×10^{-14}. *Thus, in a typical operating region with probabiliy* 10^{-5} *of word error, the probability of undetected word error is about* 10^{-19}.

I. Introduction

Deep Space missions, including Voyager, use error-correcting codes to allow very low probability of error in messages from the spacecraft to earth, even though signal-to-noise ratios are very low One of the digital coding schemes used by Voyager is shown in Fig. 1. This scheme allows a bit-error rate as low as 10^{-6} with a bit signal-to-noise ratio E_b/N_0 as low as 2 3 dB.

Besides low decoder bit-error rate, we would like a system with very low probability of undetected error. That means that, in case there are bit errors in a certain region, we would like to know that. (Of course, knowing exactly where the bit errors are is equivalent to having no bit errors, which is impossible. But we would like to know that a certain string of bits contains errors or, preferably, that it is very unlikely to contain errors.)

Our Reed-Solomon code is a (255,223) 8-bit code. This means that bits are arranged in symbols of 8 bits each, which are in turn arranged in words of 255 symbols, of which 223 symbols are information and the other 32 are parity. Whenever our decoders detect 16 or fewer symbol errors, they correct these errors. But if the string going into the decoder differs from *every* codeword in at least 17 symbols, we are able to detect this, and we know that many symbols (and therefore many bits) in the word are in error. We would like to know the probability that, in the fairly rare instance that 17 or more symbol errors are made, the decoder makes further correction and therefore incorrectly reports successful decoding. This article shows that this probability is less than 3×10^{-14}.

Let C be an (n, k) code over $GF(q)$, with minimum distance d. We assume C is being used to correct t errors, where t is a fixed integer satisfying $2t \leqslant d - 1$. We further assume the decoder is a *bounded distance* decoder, i.e., it looks for a codeword within distance t of the received word; if there is such a codeword, the decoder finds it, and if not, the decoder reports "failure."

If the transmitted codeword suffers t or fewer errors, it will be decoded correctly. If, on the other hand, it suffers more than t errors, one of two things can happen. Either the decoder will fail to find a codeword (*decoder failure*), or it will find a codeword other than the transmitted codeword (*decoder error*). We denote by P_F and P_E the probabilities of decoder failure and error, respectively. Of course if the number of errors is t or less, $P_F = P_E = 0$. If the number of errors exceeds t, but is less than $d - t$, then $P_F = 1$ and $P_E = 0$, since fewer than $d - t$ errors occuring cannot move the transmitted codeword to within distance t of another codeword.

If $d - t$ or more errors occur, it is in general quite difficult to calculate, or even estimate, P_F and P_E, although if the code is being used in a practical communications system, it is important to do so. A useful heuristic estimate can be based on the assumption that if at least $d - t$ errors occur, the error pattern can be treated as if it were *completely random*. The probability that a completely random error pattern will cause decoder error (i.e., lie within distance t of a nonzero codeword) is given by

$$Q = \frac{(q^k - 1) \cdot V_n(t)}{q^n} = (q^{-r} - q^{-n}) V_n(t) \qquad (1)$$

where $r = n - k$ is the code's redundancy and

$$V_n(t) = \sum_{s=0}^{t} \binom{n}{s} (q - 1)^s \qquad (2)$$

is the volume of a Hamming sphere of radius t This argument leads to the following estimate for P_E ·

$$P_E \approx Q \cdot \Pr\{\geqslant d - t \text{ errors}\} \qquad (3)$$

It is difficult to justify this estimate in general, but in this article we will see that if we increase Q slightly by defining Q' as

$$Q' = (q - 1)^{-r} V_n(t) \qquad (4)$$

then for Reed-Solomon codes,

$$P_E \leqslant Q' \cdot \Pr\{\geqslant d - t \text{ errors}\} \qquad (5)$$

In fact Eq (5) will follow from more detailed results, which we now describe.

If q_u denotes the probability that the error pattern has weight u, then plainly

$$P_E = \sum_{u=0}^{n} P_E(u)\, q_u \qquad (6a)$$

$$P_F = \sum_{u=0}^{n} P_F(u)\, q_u \qquad (6b)$$

where $P_E(u)$ and $P_F(u)$ denote the *conditional* probabilities of decoder error and failure, respectively, given u channel errors As mentioned above, we have $P_E(u) = P_F(u) = 0$ for $u \leqslant t$ and $P_E(u) = 0, P_F(u) = 1$ for $t < u < d - t$ For $u \geqslant d - t$ we have $P_F(u) + P_E(u) = 1$, and so if $P_E(u)$ is known, $P_F(u)$ can be calculated, and vice versa.

Here is our main result. Let C be an (n, k) Reed-Solomon, or any other maximum distance separable (MDS) code, with minimum distance $d = n - k + 1$ We assume as above that the code is being used to correct t errors, for some fixed value of t with $2t \leqslant d - 1$ We further assume that the code is being used on a channel for which all error patterns of the same weight are equiprobable, for example, a q-ary symmetric channel. Under these assumptions, we shall prove in Section III that

$$P_E(u) = 0 \qquad \text{for } u \leqslant d - t - 1 \qquad (7a)$$

$$P_E(u) \leqslant (q - 1)^{-r} \sum_{s=d-u}^{t} \binom{n}{s} (q - 1)^s \qquad \text{for } d - t \leqslant u \leqslant d - 1 \qquad (7b)$$

$$P_E(u) \leqslant Q' \qquad \text{for } u \geqslant d \qquad (7c)$$

Of course Eq. (7a) needs no further proof; it is included only to make the bounds in Eq. (7) apply to all values of u. The bound (7b) actually follows from a slightly sharper, but more complicated bound on $P_E(u)$ that appears in Section III as Eq. (15).

We can combine Eqs (7b) and (7c), at the cost of weakening Eq. (7b) slightly, to obtain an upper bound on $P_E(u)$ which is uniform in u for $u \geqslant d - t$:

$$P_E(u) \leqslant Q' \qquad \text{for } u \geqslant d - t \tag{8}$$

The ratio of this uniform bound Q' to the heuristic estimate Q in Eq. (1) is usually very close to 1, and is always less than $(q/(q-1))^n$, which for $n \leqslant q - 1$ cannot exceed $e = 2.718 \ldots$. In any event, combining Eq. (6a) with (7a) and (8), we obtain the bound (5).

Although as a practical matter it is not hard to compute the bound Q' numerically, for some applications it may be worthwhile to have a simpler, though weaker, bound In the Appendix, we show that Eq. (8) implies that provided $n \leqslant q - 1$, for all $u \geqslant d - t$,

$$P_E(u) \leqslant \begin{cases} \dfrac{1}{(q-1)^{r-2}} + \dfrac{1}{(q-1)^r} & \text{if } t = 1 \\[2ex] \dfrac{1}{(q-1)^{r-2t}} \cdot \dfrac{1}{t!} & \text{if } t \geqslant 2 \end{cases} \tag{9}$$

Since $r \geqslant 2t$ in all cases, Eq (9) implies, whenever $n \leqslant q - 1$,

$$P_E(u) \leqslant \frac{1}{t!} \qquad \text{for all } u \geqslant t + 1 \tag{10}$$

Kasami and Lin (Ref. 2) have also studied the problem of decoder error for Reed-Solomon codes. They showed that on a q-ary symmetric channel P_E is at most Q, i.e., that

$$\sum_{u=d-t}^{n} P_E(u) \binom{n}{u} \epsilon^u (1-\epsilon)^{n-u} \leqslant Q \tag{11}$$

where ϵ is the probability of channel symbol error. They further showed that $P_E = Q$ only when $\epsilon = (q-1)/q$, i.e., when the error pattern is completely random. This shows that Q is the tightest possible bound on the sum in Eq. (11) which is independent of ϵ. However, except when the probabilitity of $\geqslant d - t$ errors is very nearly 1, our bound (5) will be smaller than Kasami and Lin's bound (11). And since most well-designed systems will have $\Pr\{u \geqslant d - t\} \ll 1$, we conclude that our bound is likely to be more useful in practice than Kasami and Lin's.

Finally we note that since with $\epsilon = (q-1)/q$ equality holds in Eq. (11), the *average* of the $P_E(u)$'s with respect to one particular probability distribution is Q. Since $P_E(u)$ is 0 for $u < d - t$, it follows that for some values of $u, P_E(u) > Q$. Thus the conjecture that $P_E(u) \leqslant Q$ for all u isn't tenable. (It would be nice to have a uniform *lower* bound on the $P_E(u)$'s, but we have been unable to find one.)

II. Preliminaries

In this section we will review some known results about MDS codes which are needed in our proof. Our remarks will be self-contained, but proofs may also be found in Ref. 4, Chapter 11.

Let **C** be a code, not necessarily linear, of length n with q^k codewords over $GF(q)$. If we examine any set of $k - 1$ components of the codewords, we find that there are only q^{k-1} possibilities for the q^k codewords. Thus there must be a pair of codewords which agree on these $k - 1$ components, and so the minimum distance d of the code must satisfy $d \leqslant n - k + 1$ A code for which $d = n - k + 1$ is called a *maximum-distance separable* (MDS) code. By this definition, Reed-Solomon codes and cosets of Reed-Solomon codes are MDS codes.

Let K be a subset of k coordinate positions of an MDS code If two codewords were equal on K, the distance between them would be at most $n - k$. But this is impossible, since $d = n - k + 1$ We conclude that all q^k codewords are different on K, and so, for any possible k-tuple of elements from $GF(q)$, say $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k)$, there is a unique codeword, which, when restricted to K, equals α. This important fact we call the *basic combinatorial property* of MDS codes.

We now wish to estimate the number of codewords of weight u, for $u \geqslant d$, in an MDS code. A word of weight u must vanish on a set of $v = n - u$ coordinates. Thus let V be an arbitrary subset of v coordinates. We will estimate the number of codewords that vanish on V. Since $u \geqslant d$, then $v \leqslant k - 1$. Thus by the basic combinatorial property, if we specify that the codeword is zero exactly on V, we may specify $(k - v)$ other, nonzero, components arbitrarily. There are $(q-1)^{k-v} = (q-1)^{u-r}$ ways to do this, and so there are at most $(q-1)^{u-r}$ codewords that vanish exactly on V. Since there are $\binom{n}{v} = \binom{n}{u}$ possibilities for V, if A_u denotes the number of codewords of weight u, we have:

$$A_u \leqslant \binom{n}{u} (q-1)^{u-r} \qquad \text{for } u \geqslant d \tag{12}$$

Next we let V be a subset of v coordinate positions, where $v \geqslant k$. If we project the original code onto V, the result will be a certain (v, k) code. Since the parent (n, k) code has $d = n - k + 1$, the new code must have distance $d' \geqslant d - (n - v) = v - k + 1$. Since it is impossible for d' to be greater than $v - k + 1$, equality must hold and it follows that the projected code is a (v, k) MDS code. This simple fact will be referred to in the proof in the next section.

III. Proof of Results

We call a word, not necessarily a codeword, decodable if it lies within distance t of some codeword. If D_u denotes the number of decodable words of weight u, then for $u \geq t + 1$, we have, assuming that all error patterns of weight u are equiprobable,

$$P_E(u) = \frac{D_u}{\binom{n}{u}(q-1)^u} \tag{13}$$

Thus the problem of finding the $P_E(u)$'s is essentially the same as that of finding the weight enumerator for the set of decodable words. For example, Eq. (7c) is equivalent to

$$D_u \leq \binom{n}{u}(q-1)^{u-r} V_n(t) \qquad \text{for } u \geq d \tag{14}$$

The plan is to obtain upper bounds on D_u which will imply our various bounds on $P_E(u)$. We need to distinguish two cases, $u \geq d$ and $u \leq d - 1$.

First we assume $u \geq d$. Each decodable word can be written uniquely as $C + E$, where C is a codeword and E is a word of weight $\leq t$. For a fixed E, as C runs through the set of codewords, $\{C + E\}$ is a coset of the RS code. Since any coset of a RS code is an MDS code, by Eq (12) we know that the number of words of weight u is less than or equal to $\binom{n}{u}(q-1)^{u-r}$, since we are assuming $u \geq d$. Since the set of decodable words is the disjoint union of $V_n(t)$ cosets of the RS code, Eq (14) (and therefore Eq. [7c]) follows.

Now we assume that $u \leq d - 1$. A decodable word of weight u will vanish on a set of size $v = n - u$. For each of the $\binom{n}{u}$ subsets V of v coordinates, we will obtain an upper bound on the number of decodable words of weight u that vanish on V. This upper bound will imply Eq. (7b).

As before, we will use the fact that each decodable word is of the form $C + E$, where C is a codeword and E has weight $\geq t$. If the sum $C + E$ vanishes on V, then C must have weight $\leq t$ on V, say weight w. We note that $w = 0$ isn't possible, since $u \geq t + 1$. By our remarks in Section II, we know that C restricted to V is a linear (v, k) MDS code, and so its minimum weight (distance) is $d - u$. Thus w, the weight of C on V, satisfies $d - u \leq w \leq t$. (If $d - u > t$, there are no such words, this gives another proof of Eq. [7a].) By Eq. (12), it follows that the number of codewords with weight w on V is at most $\binom{v}{w}(q-1)^{w-r'}$, where $r' = r - u$ is the redundancy of the restricted code.

For each codeword C with weight w in V, we must count the number of E's such that $C + E$ vanishes on V. Suppose that E has weights $s \geq w$. On V, E must match C exactly, but the $(s - w)$ other nonzero components can be arbitrarily placed outside V Thus the total number of E's, for a given C of weight w, is

$$\sum_{s=w}^{t} \binom{u}{s-w}(q-1)^{s-w}$$

Therefore the total number of decodable words vanishing on V is at most

$$\sum_{w=d-u}^{t} \binom{v}{w}(q-1)^{w-r'} \sum_{s=w}^{t} \binom{u}{s-w}(q-1)^{s-w}$$

$$= (q-1)^{-r'} \sum_{s=d-u}^{t} (q-1)^{s} \sum_{w=d-u}^{s} \binom{v}{w}\binom{u}{s-w}$$

This is a bound on the number of decodable words of weight u vanishing on V. If we multiply it by the number of possible subsets V with v elements, viz. $\binom{n}{v} = \binom{n}{u}$ we obtain a bound on D_u, and hence by Eq. (13),

$$P_E(u) \leq (q-1)^{-r} \sum_{s=d-u}^{t} (q-1)^{s} \sum_{w=d-u}^{s} \binom{v}{w}\binom{u}{s-w} \tag{15}$$

This bound is a bit clumsy for everyday use, but we note in passing that for $u = d - t$ (the smallest value of u for which $P_E(u)$ isn't 0) it simplifies to

$$P_E(d-t) \leq (q-1)^{-(d-t-1)} \binom{n-d+t}{t} \tag{16}$$

which is in fact the exact value of $P_E(u)$ in this case (Ref. 1).

Finally, we simplify the bound (15) by recalling a well-known combinatorial identity (Ref. 3, Eq. [1.2.6 21]):

$$\sum_{w \geq 0} \binom{v}{w}\binom{u}{s-w} = \binom{v+u}{s}$$

Since $\nu + u = n$, this means that the inner sum in Eq (15) is at most $\binom{n}{s}$, and so Eq. (7b) follows from Eq. (15).

IV. Numerical Results

Using Eq. (8) we are able to compute an upper bound to the probability of undetected error, given that a word has more than t errors. In the case of the Voyager Reed-Solomon code, this gives an upper bound of 2.97×10^{-14}. Better bounds depend on knowing the error probability so that the expected number of errors can be taken into account For example, the probability of undetected error, given that a word has exactly 17 errors (the smallest number that the code is unable to decode correctly) is $1\ 09 \times 10^{-14}$ (see Eq. [16]). This means that at a low error rate, when most words which fail to decode have exactly 17 errors, the probability of undetected word error given that a word fails to decode correctly, can be as low as 1.1×10^{-14}. In any case, we have very good confidence in those words which do decode.

References

1. Berlekamp, E. R., and Ramsey, J. L., "Readable Erasures Improve the Performance of Reed-Solomon Codes," *IEEE Trans. Inform. Theory*, Vol. IT-24, pp. 632–633, Sept. 1978

2. Kasami, T., and Lin, S., "On the Probability of Undetected Error for the Maximum Distance Separable Codes," *IEEE Trans. Comm.*, Vol. COM-32, pp. 998–1006, Sept 1984.

3. Knuth, D. E., *The Art of Computer Programming, Vol. 1, Fundamental Algorithms*. Reading, Mass., Addision-Wesley, 1968.

4. MacWilliams, F J., and Sloane, N. J. A., *The Theory of Error-Correcting Codes*. Amsterdam, North Holland, 1977.

5. Peterson, W. W., *Error-Correcting Codes*. New York, Wiley-M.I.T. Press, 1961.

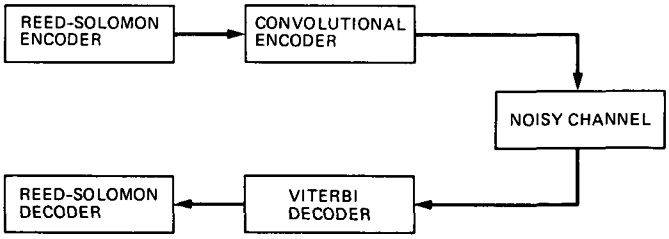

Fig. 1. A digital data coding scheme

Appendix

In this appendix we will derive several useful approximations to the bound Q' that appears in Eq. (8). In fact all of our results will follow from bounds on the binomial sum $V_n(t)$ defined in Eq. (2).

It follows from results in Ref. 5 (Appendix A, Eqs. [A-5] and [A-9]) that

$$V_n(t) \leqslant \left\{ \frac{(n-t)(q-1)}{(n-t)q-n} \right\} \binom{n}{t} (q-1)^t \qquad \text{(A-1)}$$

provided the denominator within the braces is positive. (This will certainly be the case in our application, since $2t + 1 \leqslant n$ and $q \geqslant 2$.) Now if we assume that $n \leqslant q$ (which holds for all RS codes and all but a few exotic MDS codes described in Chapter 11 of Ref. 4), the term within the braces will be $\leqslant (n+1)/n$. Thus we have

$$V_n(t) \leqslant \frac{n+1}{n} \binom{n}{t} (q-1)^t \qquad \text{(A-2)}$$

Since $(n+1)(n-1) < n^2$, it follows from Eq. (A-2) that

$$V_n(t) \leqslant \frac{n^t}{t!} (q-1)^t, \qquad \text{for } t \geqslant 2 \qquad \text{(A-3)}$$

If $n \leqslant q - 1$, the bound (A-3) immediately implies Eq. (9) for $t \geqslant 2$. The case $t = 1$ in Eq. (9) must be handled separately, and follows from the fact that $V_n(1) = 1 + n(q-1)$ is less than or equal to $1 + (q-1)^2$, if $n \leqslant q - 1$.