Detection and correction of multiple errors in general block codes

EGGHE, Leo (1999) Detection and correction of multiple errors in general block codes. In: Mathematical and Computer Modelling, 30(7-8). p. 113-121.

DOI: 10.1016/S0895-7177(99)00169-7
Handle: http://hdl.handle.net/1942/793

DETECTION AND CORRECTION OF MULTIPLE ERRORS IN GENERAL BLOCK CODES

by

L. EGGHE

LUC, Universitaire Campus, B-3590 Diepenbeek, Belgium[1]
and
UIA, Universiteitsplein 1, B-2610 Wilrijk, Belgium

ABSTRACT

The paper deals with general block codes where the symbol sets at each coordinate do not have to be the same. First of all the classical Hamming bound inequality for error correcting systems, is extended to this case.

Next a new necessary condition for systems, able to detect all 1,...,2k-1 errors ($k \in \mathbb{N}$) is proved. From this a new bound for such systems is proved. All results are proved to be optimal.

The results have applications e.g. in ISBN (International Standard Book Number) or ISSN (International Standard Serial Number) - like systems.

[1]Permanent address

Keywords and phrases : error detection, error correction, block code, Hamming bound.
Acknowledgement : the author is indebted to Prof. Dr. R. Rousseau for interesting discussions on the content of this paper.

I. Introduction

Block codes can, simply, be defined as follows (see e.g. van Tilborg (1993), Pretzel (1992)). Let

$$\Omega = \prod_{i=1}^{n} M_i \quad , \tag{1}$$

where M_i denote n (possibly different) finite sets. Any element

$$x_1 x_2 \ldots x_n \in \Omega$$

is called a possible block code. Note that

$$|\Omega| = \prod_{i=1}^{n} |M_i| \tag{2}$$

where $|.|$ denotes the cardinality of the set. We will denote $m_i = |M_i|$ (i=1,...,n).

Examples of block codes.

1. Classical ISSN or ISBN-framework (ISSN = International Standard Serials Number, ISBN = International Standard Book Number), using 11-multiples (see further)

$$M_1 = \ldots = M_7 = \{0,\ldots,9\}$$
$$M_8 = \{0,\ldots,9,X\} \text{ (ISSN)}$$
$$M_1 = \ldots = M_9 = \{0,\ldots,9\}$$
$$M_{10} = \{0,\ldots,9,X\} \text{ (ISBN)}$$

   See Hill (1986).

2. System where one uses 13-multiples instead of 11 as above. Now

$$M_8 = \{0,\ldots,9,X,Y,Z\} \text{ (ISSN)}$$
$$M_{10} = \{0,\ldots,9,X,Y,Z\} \text{ (ISBN)}$$

   respectively.

3. System with 2 check digits based on 11-resp. 13-multiples (e.g. for ISBN) :

$$M_1 = \ldots = M_9 = \{0,\ldots,9\}$$
$$M_{10} = \{0,\ldots,9,X\}$$
$$M_{11} = \{0,\ldots,9,X,Y,Z\}$$

4. Note that we do not suppose that our system works with check digits. Very generally we can put (1) and determine later what we will consider as correct codes

Let $A \subset \Omega$ be the set of correct codes. They are defined by the system. We do not suppose any system here.

Examples of correct codes in block code systems.

1. In the examples 1,2,3 above the device to be in A is by making multilinear combinations of the x_i s and where one checks if we have an 11-multiple (resp. a 13-multiple) - see e.g. Hill (1986), Egghe (1985), Mc Murdo (1981), Mac Cormack (1982) or the recent Egghe and Rousseau (1998).

   For a general description of ISBNs and ISSNs, we refer the reader to Mc Queen (1993). Note that the future length (n) of ISBNs or ISSNs will increase due to the electronic publishing phenomenon - see Simmons (1997).

2. In case of example 4 (for $M_i = \{0,\ldots,9\}$, i=1,...,n), a correct code could be one for which $x_1\ x_2\ \ldots\ x_n \in \Omega$ could be written as (points denote consecutive numbers and are not multiplications)

$$x_1 \ldots x_{i_1}\ x_{i_1+1} \ldots x_{i_2} \ldots x_{i_{j-1}+1} \ldots x_{i_j}$$

   (where $i_j=n$) such that

$$\sum_{k=1}^{j} (x_{i_{k-1}+1} \ldots x_{i_k})^2 \qquad (3)$$

   is a complete square (the so-called generalized Pythagorean numbers) (take $i_0=1$). Example : n=2, then $34 \in A$ since $3^2+4^2=5^2$ and $24 \in \Omega \setminus A$ since $2^2+4^2=20$ and since $\sqrt{20} \notin \mathbb{N}$. Note that such examples of two natural numbers (whose sum of squares is again a square) can only be given for squares. Indeed, recently, the more than three hundred year old problem of Fermat (called the last "theorem" of Fermat) is solved by Wiles (see Wiles (1995) for a brief description of the elaborate proof or Singh (1997) for a historical review) resulting in the fact that no numbers x,y and $z \in \mathbb{N}$ exist for which $x^k+y^k=z^k$, $k \in \mathbb{N}$, $k \geq 3$. But equations as $x^k+y^k+z^k=u^k$ ($x,y,z,u,k \in \mathbb{N}$, $k \geq 3$) are possible (see Singh (1997), p. 178).

3. In Krishna, Krishna, Lin and Sun (1994) one studies RNS (Residue Number Systems). Here one takes n pairwise relatively prime numbers $p_1,...,p_n$ and a correct code $X=x_1...x_n$ is obtained iff $x_i=X \pmod{p_i}$ for a (unique - by the Chinese Remainder Theorem) number $X\in[0,p[$, where $p=\prod_{i=1}^{n} p_i$. Algorithms to find X are available, see e.g. Krishna and Sun (1993). Many variants of the above described RNS exist (again see the above mentioned references).

Note in the above examples that the sets M_i can be different for $i\in\{1,...,n\}$. In Pretzel (1992) and van Tilborg (1993) only block codes with fixed symbol sets are studied. Therefore an extension of the results (e.g. on the Hamming bound - see van Tilborg (1993)) is necessary. Hereby we are not only interested in error correcting systems but also in (the weaker) error detecting systems. In the latter case our results will also be new in case the symbol set remains fixed.

Let us first repeat, in our general framework, what we mean by a k-error correcting or k-error detecting system ($k\in\mathbb{N}$).

Let $A_k\subset\Omega$ ($k\in\mathbb{N}$) be the set of all codes such that $\forall Y\in A_k$, $\exists X\in A$ such that X and Y differ at k places. Note that k equals the Hamming distance d(X,Y) between X and Y.

Let $X\in A$. Denote by $B_k(X)$ the set of all codes Y such that X and Y differ at k places. Obviously

$$A_k = \bigcup_{X\in A} B_k(X) \tag{4}$$

Definition I.1 : We say that the system detects all k-errors iff

$$A_k \cap A = \varnothing \tag{5}$$

Definition I.2 : We say that the system corrects all k-errors iff

$$\{B_k(X) \| X\in A\} \tag{6}$$

forms a partition of $A_k\backslash A$.

One can readily see that these definitions agree with the classical notions of detection and correction, although the above definitions seem new to us. Indeed, (5) says that no k-error can be correct and hence is detected. (6) says that any k-error leads uniquely to the one $X \in A$ that differs in k places with the given code. Note that definition 2 implies $A_k \cap A = \varnothing$, hence definition 1.

The following result is very easy in this framework :

Theorem I.1 : If the system detects all 1,2,...,2k-errors ($k \in \mathbb{N}$ fixed), then it corrects all 1,2,...,k-errors.

Proof : Let $i \in \{1,...,k\}$. Suppose $\exists X, X' \in A$ such that $X \neq X'$ and such that

$$B_i(X) \cap B_i(X') \neq \varnothing.$$

Then there is a code Y differing from X in i places and differing from X′ in i places. Hence X and X′ differ in 1,2,..., or 2i places, hence $X' \in A_j$ ($\exists j \in \{1,...,2i\}$). By definition 1: $A_j \cap A = \varnothing$. Hence $X' \notin A$, a contradiction.

Since this is true $\forall i \in \{1,...,k\}$, the theorem is proved. □

Note that this result is also a consequence from the proposition on p. 17 and the one on p. 18-19 in Pretzel (1992), but the proof obtained in this way is more complicated.

The result above is false if one only supposes that the system detects all 1,2,...,2k-1-errors. Indeed, take k=1, then the statement becomes : 1-error detection implies 1-error correction which is false (take e.g. the ISBN, ISSN-systems).

Corollary I.1 : If the system detects all 1- and 2-errors then it corrects all 1-errors.

Application : If we calculate 2-check-digits for ISSNs or ISBNs (e.g. by using 11 and 13 as divisors, cf. example 3) then it is easy to see that it detects all 1- and 2-errors (exercise) (cf. also Egghe and Rousseau (1998)), hence by the above corollary, this system corrects all single errors. It takes the solution of a system of 2 linear equations (mod 11 and mod 13) to prove this directly. For k=2,3... and general

n it even takes intricate systems of linear equations to prove this! So the above theorem has far reaching applications, although its proof is very simple (because of the abstract formalism).

The above elementary remarks are the starting point for our investigations. In the next section we will calculate the values of the sets $|B_i(X)|$, yielding a generalization of the well-know Hamming bound in case of 1,...,k-correcting systems. By theorem I.1 this then also takes care of all 1,...,2k-detecting systems.

Section III then deals with the (weaker) situation where the system only detects 1,...,2k-1 errors ($k\in\mathbb{N}$). The weaker results obtained in this case are proved to be optimal so that there cannot be an improvement. The paper closes with a short section IV with examples.

II. The case of systems that are correcting 1,...,k-errors.

Note that, by theorem I.1, the results obtained in this section also apply to systems that detect 1,...,2k-errors.

Proposition II.1 : If the system corrects all 1,...,k-errors ($k\in\mathbb{N}$ fixed) then

$$\{B_i(X) \| i\in\{1,...,k\}, X\in A\},\ A \tag{7}$$

forms a partition of $\bigcup_{i=1}^{k} A_i \cup A$.

Proof : By definition, the $B_i(X)$ ($i\in\{1,...,k\}$ fixed), $X\in A$ are disjoint, but also if we let $i\in\{1,...,k\}$ vary (otherwise there would exist $i,j\in\{1,...,k\}$, $X,X'\in A$ such that

$$B_i(X) \cap B_j(X') \neq \phi$$

contradicting the fact that all i- and j-errors are corrected). □

Note that (7) implies the weaker property that all the $A_1,...,A_k$ are disjoint and disjoint from A. The weakest relaxation of the condition in proposition II.1 is to suppose that the system detects all 1,...,2k-1 errors (implying the correction of all 1,...,k-1 errors).

In this case, however, proposition II.1 is not true. Indeed, take k=1. If proposition II.1 would be true for 1,...,2k-1 error detecting systems, then this implies (by (7)) that 1-error detection implies 1-error correction ; we remarked already above that this is not true.

The above result shows that the space Ω must be pretty large since it must be able to contain all the disjoint sets in (7). If we manage to calculate the cardinality of all the sets in (7) we then obtain necessary requirements on the size of the set Ω in order to have the mentioned powers of detection and correction. This will be done now.

It is no loss of generality to assume that we can subdivide the index set $\{1,...,n\}$ as follows :

$$\{1,...,n\} = \{1,...,n_1\} \cup \{n_1+1,...,n_1+n_2\} \cup ... \cup \{\sum_{i=1}^{\ell-1} n_i+1,...,\sum_{i=1}^{\ell} n_i=n\} \qquad (8)$$

such that x_i uses p_1 symbols if $i\in\{1,...,n_1\}$, x_i uses p_2 symbols if $i\in\{n_1+1,...,n_1+n_2\}$ and so on, until : x_i uses p_ℓ symbols if i belongs to the last set. Note that we do not require the symbol sets $M_1,...,M_{n_1}$ to be equal (and the same for the other symbol sets).

This is no loss of generality since we can always rearrange $x_1...x_n$ such that the above is true (warning : by doing so we leave the number of possible codes unchanged but of course the correctness of a code is changed! - but this is not a problem here since we deal with cardinality).

Note that the above permutation of indices is not even necessary for the ISBN, ISSN codes : take e.g. the ISBN with two check digits (example 3). We have here $n_1=9$, $n_2=10$, $n_3=11$, $p_1=10$, $p_2=11$, $p_3=13$.

Proposition II.2 : Let $X\in A$, $k\in\{1,...,n\}$ be fixed but arbitrary. Then

$$|B_k(X)| = \sum_{\substack{k_1,...,k_\ell \\ \sum_{j=1}^{\ell} k_j=k}} \prod_{i=1}^{\ell} \binom{n_i}{k_i} (p_i-1)^{k_i} \qquad (9)$$

Proof : Since we look at codes $Y \in B_k(X)$, they differ at k places from $X \in A$. A k-subset of $\{1,...,n\}$ is always obtained as the disjoint union of a

$$k_1\text{-subset from } \{1,...,n_1\}$$
$$k_2\text{-subset from } \{n_1+1,...,n_2\}$$
$$...$$
$$k_\ell\text{-subset from } \{ \sum_{i=1}^{\ell-1} n_i+1, \sum_{i=1}^{\ell} n_i \},$$

such that $k=k_1+k_2+...+k_\ell$. There are respectively $\binom{n_1}{k_1},\binom{n_2}{k_2},...,\binom{n_\ell}{k_\ell}$ possible sets and in each case we have the choice of changing the correct symbols into (respectively) $(m_1-1)^{k_1},(m_2-1)^{k_2},...,(m_\ell-1)^{k_\ell}$ other ones. Hence, formula (9) is proved. □

Corollary II.1 : If the system corrects all k-errors then

$$|A|+|A_k| = |A|+|A|.|B_k(X)| \leq \prod_{i=1}^{\ell} p_i^{n_i} = \prod_{j=1}^{n} m_j = |\Omega| \qquad (10)$$

with $|B_k(X)|$ as in (9).

Proof : If the system corrects k symbols then ($\cup$ denotes the disjoint union)

$$A_k = \bigcup_{X \in A} B_k(X),$$

by definition and the fact that $A_k \cap A = \varnothing$. Hence $|A_k \cup A| = |A_k|+|A| = \sum_{X \in A} |B_k(X)|+|A| = |A|.|B_k(X)|+|A|$.

This must be less than $|\Omega| = \prod_{j=1}^{n} m_j$ (by definition) and $|\Omega| = \prod_{i=1}^{\ell} p_i^{n_i}$ (by construction). □

Corollary II.2 : If the system corrects all 1,...,k-errors (e.g. if the system detects all 1,2,...,2k-errors) ($k \in \mathbb{N}$ fixed), then

$$|A| + \sum_{i=1}^{k} |A_i| = |A| + |A| \sum_{i=1}^{k} |B_i(X)| \leq \prod_{i=1}^{\ell} p_i^{n_i} = \prod_{j=1}^{n} m_j = |\Omega| \qquad (11)$$

with $|B_i(X)|$ as in (9).

Proof : Under the above conditions, the sets in (7) are all disjoint and again

$$A_i = \dot{\bigcup}_{X \in A} B_i(X)$$

for every i=1,...,k. The rest follows as in the proof of corollary II.1. □

Note that (9), (10), (11) form a significant extension of the case in which all symbol sets are the same (or have the same number of symbols). In this case (9) becomes (ℓ=1, m_1=...=m_n=p_1=:m, n_1=n)

$$|B_k(X)| = \binom{n}{k} (m-1)^k. \tag{12}$$

In this case (10) reads

$$|A| + \sum_{X \in A} \binom{n}{k} (m-1)^k \leq m^n$$

Hence

$$|A|(1 + \binom{n}{k} (m-1)^k) \leq m^n \tag{13}$$

and (11) reads

$$|A| + \sum_{i=1}^{k} \sum_{X \in A} \binom{n}{i} (m-1)^i \leq m^n$$

or

$$|A| \cdot \sum_{i=0}^{k} \binom{n}{i} (m-1)^i \leq m^n \tag{14}$$

Inequality (14) can be read in van Tilborg (p. 13, formula (2.5)) and is called the Hamming bound. Hence (10) and (11) constitute extensions of the Hamming bounds to the case in which

the symbol sets can differ. Note that this include the ISBN and ISSN-codes, which are not included in (14)!

These generalized Hamming bounds can be used to prove that certain correction properties in certain systems cannot be obtained.

Corollary II.2 applies in the case that the system detects all 1,2,...,2k-errors. It is not true in the case the system detects all 1,2,...,2k-1 errors. Indeed take the case of the classical ISBN (k=1 here). It is easy to see that

$$A_1 = A_2 = \ldots = \Omega = \prod_{i=1}^{10} M_i,$$

where $M_1 = \ldots = M_9 = \{0,\ldots,9\}$ and $M_{10} = \{0,\ldots,9,X\}$. The reason is that the check digit detects all mistakes.

Obviously A is bijective with the set $\prod_{i=1}^{9} M_i$ (since only one value of the check digit x_{10} makes the code correct).

Hence here

$$|A_1| = |A|(m_{10}-1) \tag{15}$$

($m_{10} = 11$ in this case). Hence

$$|A| + |A_1| = |A|m_{10} = |\Omega|.$$

But (11) gives

$$|A_1| = |A| \sum_{i=1}^{n} (m_i-1) > |A|(m_{10}-1) \tag{16}$$

(n=10 here), contradicting (15). This leads us to the next section.

III. The case of systems that are detecting 1,...,2k-1-errors

In this weaker case we have the following results.

Lemma III.1 : Let $i,j \in \{1,...,n\}$ such that $i \neq j$. If the system detects all

$$|i-j|,...,i+j$$

-errors, then

$$A_i \cap A_j = \varnothing \tag{17}$$

Proof : Suppose $Y \in A_i \cap A_j$. Then there exists $X \in A$ and $X' \in A$ such that Y differs at i places from X and Y differs at j places from X'.
Hence X and X' differ at $k=|i-j|$, or ..., $k=i+j$ places. But $X \in A$, $X' \in A_k$ and $A \cap A_k = \varnothing$ by definition. Hence $X' \notin A$, a contrdiction. ■

Proposition III.1 : If the system detects all 1,2,...,2k-1-errors ($k \in \mathbb{N}$ fixed) then the $A_1,...,A_k$ are mutually disjoint (and disjoint with A).

Proof : $\forall i,j \in \{1,...,k\}$, $i \neq j$ one has $|i-j|,...,i+j \in \{1,...,2k-1\}$. Hence $A_i \cap A_j = \varnothing$ by the above lemna. That they are disjoint from A follows from the definition of i-error detectability. □

Corollary III.1 : If the system detects all 1,2,...,2k-1-errors ($k \in \mathbb{N}$ fixed) then the system is also capable of detecting the number of errors in a code.

Proof : This readily follows from the fact that the $A_1,...,A_k$ are mutually disjoint. □

Again the condition in the above proposition and corollary cannot be relaxed into "the system detects all 1,...,2k-2-errors". Indeed, take the case of an ISBN with 2 check digits, calculated

with 11 and 13 as divisors (example 3). Take k=2. Hence we have detection of 1,2=2k-2-errors (but not of all 3=2k-1-errors). Also we have that $A_1 \cap A_2 \neq \varnothing$. Indeed, take the code

$$05660351542 \in A$$

(4 is the check digit, using 11 as divisor and 2 is the check digit using 13 as divisor). Hence

$$15660351542 \in A_1$$

But if we calculate the new check digits for the partial code 156603515 we obtain 53 as check digits. Hence

$$15660351553 \in A$$

and hence

$$15660351542 \in A_2,$$

Hence $A_1 \cap A_2 \neq \varnothing$.

Based on the above results we can now prove the following theorem.

Theorem III.1 : If the system detects all 1,2,...,2k-1-errors ($k \in \mathbb{N}$ fixed), then

$$|A| + \sum_{i=1}^{k} |A_i| \leq \prod_{j=1}^{n} m_j = |\Omega| \tag{18}$$

where

$$|A_i| \geq \prod_{\ell=1}^{i} (m_{j_\ell} - 1)|A| \tag{19}$$

and where $m_{j_1},...,m_{j_i}$ are the i largest values from the set $\{m_1,...,m_n\}$. In addition, (19) is optimal in the sense that there exist systems for which equality in (19) holds.

Proof : (18) follows readily from the proposition III.1. Now the A_i's cannot be written anymore as a partition of $B_i(X)$'s as was the case in corollary II.2 but we can show the following. Let $m_{j_1},\ldots,m_{j_i}$ be the i largest numbers in $\{m_1,\ldots,m_n\}$. For every $X=x_1 \ldots x_n \in A$ we have that $Y=y_1 \ldots y_n$ where

$$\begin{cases} y_i = x_i \ , i \in \{1,\ldots,n\} \setminus \{j_1,\ldots,j_i\} \\ y_i \neq x_i \ , i \in \{j_1,\ldots,j_i\} \end{cases}$$

belongs to A_i and does not belong to A (since $A \cap A_i = \varnothing$). At each place $i \in \{j_1,\ldots,j_i\}$ there are m_i-1 different possibilities. Hence

$$|A_i| \geq \prod_{\ell=1}^{i} (m_{j_\ell} - 1)|A|.$$

This inequality is optimal in the sense that, generally, we cannot prove a higher bound. Indeed take the classical ISBN. Formula (16) shows

$$|A_1| = |A|(m_{10}-1)$$

which is, in this case, (19) but with equality sign. □

Note that this result is also new in case all the symbol sets are equal (or have an equal cardinality).

General Note : In systems where $\Omega \subset \prod_{i=1}^{n} M_i$ none of the results obtained so far are true. Let us illustrate this in relation with the previous theorem. In any case, even when $\Omega \subset \prod_{i=1}^{n} M_i$ we have, under the conditions of the above theorem (for k=1) that $|A_1| \geq |A|$. Indeed, take $X,X' \in A$, $X \neq X'$. So $\exists i \in \{1,\ldots,n\}$ such that $x_i \neq x_i'$, the values on the i th place in X resp. X'. Make the following construction : Let Y,Y' be codes where the coordinates satisfy

$$y_i \begin{cases} = x_j & (j \neq i) \\ = x_i' & (j = i) \end{cases}$$

$$y_j' \begin{cases} = x_j' & (j \neq i) \\ = x_i & (j = i) \end{cases}$$

Then since $x_i \neq x_i'$, $Y \neq Y'$. Furthermore $Y \in B_1(X)$ and $Y' \in B_1(X')$. Hence $Y, Y' \in A_1$. This shows that $|A_1| \geq |A|$. Hence we have a much weaker result than (16) or (19). Also this is optimal : take $\Omega=\{(0,0),(1,0),(1,1)\}$, and $A=\{(0,0)\}$. Then $A_1=\{(1,0)\}$, hence $|A|=|A_1|$. We even have $A_2=\{(1,1)\}$ so $|A_2|=|A|$.

But systems in which $\Omega \neq \prod_{i=1}^{n} M_i$ are not important because of the fact that, as a consequence of an error, in every coordinate (i) every symbol of the symbol set M_i can occur, hence $\Omega = \prod_{i=1}^{n} M_i$ as supposed in the beginning. Therefore we will not go into systems where $\Omega \neq \prod_{i=1}^{n} M_i$ any further.

IV. Applications.

The results obtained in the previous sections also offer necessary conditions in order to have systems that can correct k errors, 1,...,k-errors, or that can detect 1,...,k-errors (k odd or even). These can be used to show that systems do not perform this way. We give some examples.

1. Take k=1 in corollary II.2, $|A|=10^9$, $n_1=9$, $m_1=10$, $n_2=1$, $m_2=11$. Condition (11), together with (9) reads the requirement

$$10^9(1+9.9+10) \leq 10^9.11,$$

which is false. Hence <u>any</u> such system does not detect all 1,2=2k errors. Note that this fact is independent of the system. We do not even have to use a system of check digits. Of course, classical ISBN falls in this category.

2. Take k=2 in Theorem III.1, $\#A=10^9$, $n_1=9$, $m_1=10$, $n_2=1$, $m_2=11$, $n_3=1$, $m_3=13$. Conditions (18) and (19) yield the requirement

$$10^9(1+12.10.8) \leq 10^9.11.13,$$

which is false again. Hence any such system does not detect all 1,2,3=2k-1 errors. Again this fact is independent of the system (we again does not specify whether or not we use check digits). Of course ISBNs formed as in example 3 of section I fall in this category.

References

Egghe, L. (1985). A note concerning two ISBN-checking algorithms. Journal of Information Science 11, 41-42.

Egghe, L. and Rousseau R. (1998). On the detection of double errors in ISBN and ISSN-like codes. Preprint.

Hill, R. (1986). A first course in coding theory. Oxford Applied Mathematics and Computing Science Series. Clarendon Press, Oxford.

Krishna, H., Krishna, B., Lin, K.-Y. and Sun, J.-D. (1994). Computational number theory and digital signal processing. Fast algorithms and error control techniques. CRC Press, Boca Raton (Fla. USA).

Krishna, H. and Sun, J.-D.(1993). On theory and fast algorithms for error correction in Residue Number System Product Codes. IEEE Transactions on Computers 42(7), 840-853.

MacCormack, J.A.D. (1982). Letter to the editor. Journal of Information Science 5, 172.

McMurdo, G. (1981). An alternative ISBN checking algorithm. Journal of Information Science 3, 235-237.

McQueen, J. (1993). Record matching : ISBNs and ISSNs. Information Today, 48-49.

Pretzel, O. (1992). Error-correcting codes and finite fields. Oxford Applied Mathematics and Computing Science Series, Clarendon Press, Oxford.

Simmons, A. (1997). The 21st century ISBN. The Bookseller (5 December 1997), 20-22.

Singh, S. (1997). Fermat's last theorem. The story of a riddle that confounded the world's greatest minds for 358 years. Fourth Estate, London.

Van Tilborg, H. (1993). Error-correcting codes - a first course. Student-litteratur and Chartwell Bratt, Lund.

Wiles, A. (1995). Modular forms, elliptic curves and Fermat's last theorem. Proceedings of the International Congress of Mathematicians (Zürich, 1994), 243-245. Birkhauser, Basel.