International Standard ISO 7064

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION•МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ•ORGANISATION INTERNATIONALE DE NORMALISATION

Data processing — Check character systems

Traitement des données — Systèmes de caractères de contrôle

First edition — 1983-09-15

UDC 681.3.071 **Ref. No. ISO 7064-1983 (E)**

Descriptors : data processing, character sets, control characters, numerical control, specifications.

ISO 7064-1983 (E)

Price based on 13 pages

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of developing International Standards is carried out through ISO technical committees. Every member body interested in a subject for which a technical committee has been authorized has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work.

Draft International Standards adopted by the technical committees are circulated to the member bodies for approval before their acceptance as International Standards by the ISO Council.

International Standard ISO 7064 was developed by Technical Committee ISO/TC 97, *Information processing systems*, and was circulated to the member bodies in November 1981.

It has been approved by the member bodies of the following countries :

Belgium	Germany, F. R.	South Africa, Rep. of
China	Ireland	Spain
Czechoslovakia	Italy	Sweden
Denmark	Japan	Switzerland
Egypt, Arab Rep. of	Netherlands	United Kingdom
Finland	Poland	USA
France	Romania	

No member body expressed disapproval of the document.

Printed in Switzerland

Data processing — Check character systems

0 Introduction

The need for standardization of check character systems was determined by the following considerations :

a) of the 100 or more systems in use, many have very similar characteristics, and much of the variety does not provide any significant benefit;

b) few of the existing systems have been thoroughly verified mathematically and several have serious defects;

c) the variety of systems undermines the economics of products which generate or validate check characters, and frequently prevents the checking of interchanged data.

Therefore a small set of compatible systems has been selected to cope with various application needs; they have been validated, and within the constraints of each application, offer high protection against typical transcription and keying errors.

Existing check character systems as specified in ISO 2108, ISO 2984 and ISO 6166 are used in special application fields. These do not however, achieve the error detection rate of the systems specified in this International Standard.

Annex A summarizes the criteria to be considered when selecting a check character system specified in this International Standard for a particular application.

Annex B illustrates how further compatible national check character systems may be developed for national alphabets having a different number of letters from the 26-letter internationally used alphabet for which the check character systems in this International Standard are designed.

1 Scope and field of application

1.1 This International Standard specifies a set of check character systems capable of protecting strings against errors which occur when people copy or key data. The strings may be of fixed or variable length and may have character sets which are

a) numeric (10 digits : 0 to 9);

b) alphabetic (26 letters : A to Z);

c) alphanumeric (letters and digits).

Embedded spaces and special characters are ignored.

1.2 This International Standard specifies conformance requirements for products described as generating check characters or checking strings using the systems given in this International Standard.

1.3 These check character systems can detect :

a) all single substitution errors (the substitution of a single character for another, for example 4234 for 1234);

b) all or nearly all single transposition errors (the transposition of two single characters, either adjacent or with one character between them, for example 12354 or 12543 for 12345);

c) all or nearly all shift errors (shift of the whole string to the left or right, for example

[1 2 3] for [1 2 3]);

d) a high proportion of double substitution errors (two separate single substitution errors in the same string, for example 7234587 for 1234567);

e) a high proportion of all other errors.

1.4 This International Standard excludes systems designed specifically to :

a) permit both error detection and automatic correction;

b) detect deliberate falsification;

c) check strings interchanged solely between machines.

1.5 This International Standard is for use in information interchange between organizations; it is also strongly recommended as good practice for internal information systems.

Section one : General

2 Definitions

2.1 check character : Added character which may be used to verify the accuracy of the string through a mathematical relationship to that string.

2.2 check character system : Set of rules for generating check characters and checking strings incorporating check characters.

2.3 supplementary character; supplementary check character : Check character which does not belong to the character set of the strings which are to be protected.

2.4 modulus : Integer used as a divisor of an integer dividend in order to obtain an integer remainder.

2.5 congruence : Property of a set of integers which differ from each other by a multiple of the modulus. Congruence is indicated by the symbol $\equiv$. For example, $39 \equiv 6 \pmod{11}$ indicates that 39 and 6 are congruent with respect to the modulus 11, i.e. $39 - 6 = 33$, which is a multiple of 11.

2.6 radix : Base of a geometric progression.

3 Types of systems

This International Standard specifies two types of systems :

a) pure systems;

b) hybrid systems.

3.1 Pure systems

The pure systems are listed in table 1 and specified in section two. They each use a single modulus for all stages of the calculation.

3.2 Hybrid systems

The hybrid systems are listed in table 2 and specified in section three. The hybrid systems each use two moduli in the calculation. One modulus is equal to, and the other is one greater than, the number of characters in the character set of the string to be protected. These hybrid systems always provide a check character within the character set of the string to be protected.

Table 1 — Pure systems

Check character system designation[1)]	Application	Number and type of check characters[2)]
ISO 7064, MOD 11-2	Numeric strings	1 digit or the supplementary character X
ISO 7064, MOD 37-2	Alphanumeric strings	1 digit or letter or the supplementary character ✲
ISO 7064, MOD 97-10	Numeric strings	2 digits
ISO 7064, MOD 661-26	Alphabetic strings	2 letters
ISO 7064, MOD 1271-36	Alphanumeric strings	2 digits or letters

1) The first number following "MOD" in the designation is the modulus and the second number is the radix.

2) The first two systems may produce a supplementary check character outside the character set of the string to be checked (i.e. ISO 7064, MOD 11-2 check characters are 0 to 9 plus X, and ISO 7064, MOD 37-2 check characters are 0 to 9, and A to Z, plus ✲). Where the supplementary check character is not acceptable and a single check character is required, it may be possible to avoid issuing those strings which yield the supplementary character. If neither the supplementary check character can be tolerated nor can the strings yielding it be avoided, then the hybrid systems may be used instead.

Table 2 — Hybrid systems

Check character system designation[1)]	Application	Number and type of characters
ISO 7064, MOD 11, 10	Numeric strings	1 digit
ISO 7064, MOD 27, 26	Alphabetic strings	1 letter
ISO 7064, MOD 37, 36	Alphanumeric strings	1 digit or letter

1) The two numbers following "MOD" in the designation are the two moduli.

4 Compliance and designation

4.1 Strings

Strings protected by one of the systems specified in this International Standard for the relevant application comply with this International Standard.

4.2 Check character generating products

4.2.1 Products (which may be software or hardware) which are described as generating check characters to this International Standard without further qualification shall be capable of generating check characters for all systems in this International Standard.

4.2.2 The description of products which do not generate check characters for all the systems in this International Standard shall specify those systems which they do cover, for example "generates check characters for ISO 7064, MOD 11-2".

4.3 Checking products

4.3.1 Products (which may be software or hardware) which are described as checking strings to this International Standard without further qualification shall be capable of using all the systems in this International Standard.

4.3.2 The description of products which check strings using only certain of the systems in this International Standard shall specify those systems which they do cover, for example "checks strings using ISO 7064, MOD 11-2".

4.4 System designation

4.4.1 Normally the full designation of each system as given in tables 1 and 2 shall be used, for example "ISO 7064, MOD 11-2".

NOTE — Abbreviation to forms such as "MOD 11" will create confusion with the similar systems using modulus 11.

4.4.2 Where there is a special need for brevity, for example when it is necessary to accompany a transmitted data element by an indication of the system used to protect it, the following single digit designations may be used :

Check character system	Designation
ISO 7064, MOD 11-2	1
ISO 7064, MOD 37-2	2
ISO 7064, MOD 97-10	3
ISO 7064, MOD 661-26	4
ISO 7064, MOD 1271-36	5
ISO 7064, MOD 11,10	6
ISO 7064, MOD 27,26	7
ISO 7064, MOD 37,36	8
No check character or non-standard system	0

Section two : Pure systems

5 Specification of pure systems

5.1 Formula

A character string satisfies the check when :

$$\sum_{i=1}^{n} [a_i \times r^{(i-1)}] \equiv 1 \pmod{M}$$

where

n is the number of characters in the string, including check character(s);

i is the index of the character position starting from the right (i.e. for the rightmost character, $i = 1$), disregarding spaces and separators;

a_i is the value of the character in position i as defined in table 3;

r is the radix (i.e. the base for the geometric progression);

M is the modulus.

5.2 Calculation

Any calculation procedure which satisfies the formula may be used.

5.3 Check character position

The check character(s) shall be placed at the rightmost end of the string.

Table 3 — Values assigned to characters

Character	Value in systems for numeric strings	Value in systems for alphabetic strings	Value in systems for alphanumeric strings
0	0		0
1	1		1
2	2		2
3	3		3
4	4		4
5	5		5
6	6		6
7	7		7
8	8		8
9	9		9
supplementary character X for ISO 7064 MOD 11-2	10		
A		0	10
B		1	11
C		2	12
D		3	13
E		4	14
F		5	15
G		6	16
H		7	17
I		8	18
J		9	19
K		10	20
L		11	21
M		12	22
N		13	23
O		14	24
P		15	25
Q		16	26
R		17	27
S		18	28
T		19	29
U		20	30
V		21	31
W		22	32
X		23	33
Y		24	34
Z		25	35
supplementary character * for ISO 7064 MOD 37-2			36

6 Computational methods for pure systems with one check character

There are two basic computational methods for the pure systems. These are the *pure system recursive method* and the *pure system polynomial method*. Both yield the same result.

6.1 Pure system recursive method

6.1.1 Computation

In the recursive method the string is processed character by character from left to right.

With the index $j = 1 \ldots n$ where n is the number of characters in the string including the check character, and defining $P_j = 0$ for $j = 1$, calculate :

$$S_j = P_j + a_{(n-j+1)}$$

$$P_{(j+1)} = S_j \times r$$

where

$a_{(n-j+1)}$ is the character value;

r is the radix.

For checking purposes the string is taken as correct if

$$S_n \equiv 1 \pmod{M}$$

When generating a check character a_1 shall be chosen so that

$$P_n + a_1 \equiv 1 \pmod{M}$$

6.1.2 Example

Assume that the string 0794 is to be provided with a check character using the check character system ISO 7064, MOD 11-2.

Here $M = 11$, $r = 2$ and $n = 5$ (i.e. 4 characters plus 1 check character).

The calculation may then be set out as below.

Step	Product brought forward	+	Next character value	=	Intermediate sum (see note 1)	Intermediate sum	×	Radix	=	Product carried forward (see note 1)
j	P_j	+	$a_{(n-j+1)}$	=	S_j	S_j	×	r	=	$P_{(j+1)}$
1	0	+	0	=	0	0	×	2	=	0
2	0	+	7	=	7	7	×	2	=	14
3	14	+	9	=	23	23	×	2	=	46
4	46	+	4	=	50	50	×	2	=	100
5	100	+ check character value is to be congruent to 1 (mod 11)								

The final product is P_n, here 100. This plus the check character value is to be congruent to 1 (mod 11). As 100 is itself congruent to 1 (mod 11), the check character value must be zero, and the full protected string is 07940, the check character being appended to the right of the string.

To check the string, the steps $j = 1$ to 5 above are computed as shown, but with the check character value, 0, being included in the calculation; if the result is congruent to 1 (mod 11) the string is accepted as valid.

NOTES

1 If at any stage the product $P_{(j+1)}$ or the sum S_j is greater than the modulus M, multiples of the modulus may be discarded and the integer remainder be used for further calculations. In the calculations above :

$P_3 = 14$ but could be $14 - 11 = 3$

$S_3 = 23$ but could be $23 - 22 = 1$

$P_4 = 46$ but could be $46 - 44 = 2$

2 The valid check character values in the system ISO 7064, MOD 11-2 are zero to 10. If the value of the check character is 10, it is represented by the character "X". If the original string had been the shorter string 079 :

then at the end of step 3 the value is 46;

$46 \equiv 2 \pmod{11}$;

as $2 + 10 \equiv 1 \pmod{11}$ the complete string is 079<u>X</u>.

To verify the string after step 3 we would have $46 + 10 = 56$, which is congruent to 1 (mod 11), thus satisfying the check.

6.2 Polynomial method

6.2.1 Computation

The polynomial method for the pure systems is computed by multiplying the value for each character in the string by $r^{(i-1)}$ or by $r^{(i-1)} \pmod{M}$. A list of the first fifteen values of $r^{(i-1)} \pmod{M}$ for all the pure systems is given in table 4.

Multiply the character values by their weights; add the products. Strings including the check character are valid if the sum of these products is congruent to 1 (mod M).

6.2.2 Example

The computation to generate the check character by the polynomial method for the same string used in the example in 6.1.2, i.e. 0794, is :

Character position i :	5	4	3	2	1
Weight $2^{(i-1)} \pmod{11}$	5	8	4	2	1
Character value a_i :	0	7	9	4	
Products :	0	56	36	8	
Sum of products :	0 + 56 + 36 + 8 = 100				

This sum, here 100, plus the check character value must be congruent to 1 (mod 11). As 100 itself is congruent to 1 (mod 11), the check character value must be zero, and the full protected string is 0794<u>0</u>, the check character being appended to the right of the string.

To check the string with this method, multiply each character value (including the check character value) by the weight associated with its position; sum the products and divide by 11 to get the integer remainder. If this is 1 the check is satisfied.

Character position i :	5	4	3	2	1
Weight $2^{(i-1)} \pmod{11}$	5	8	4	2	1
Character values a_i :	0	7	9	4	0
Products :	0	56	36	8	0
Sum of the products :	0 + 56 + 36 + 8 + 0 = 100				

$= 100 \equiv 1 \pmod{11}$

thus satisfying the check.

NOTE — The rightmost position, i.e. the position with the weight $r^0 = 1$, is reserved for the check character, so the rightmost position of the original string (*without* the check character) is associated with a weight of r, here 2.

Table 4 — Pure system weights

Position index	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
ISO 7064, MOD 11-2	5	8	4	2	1	6	3	7	9	10	5	8	4	2	1
ISO 7064, MOD 37-2	30	15	26	13	25	31	34	17	27	32	16	8	4	2	1
ISO 7064, MOD 97-10	53	15	50	5	49	34	81	76	27	90	9	30	3	10	1
ISO 7064, MOD 661-26	129	488	273	341	547	199	389	498	70	562	225	390	15	26	1
ISO 7064, MOD 1271-36	769	904	590	87	532	156	428	718	373	893	625	900	25	36	1

NOTE — Weights are shown for the first fifteen positions only. The series can be extended indefinitely, using the formula

$$w_i = r^{(i-1)} \pmod{M}$$

where w_i is the weight for position i.

7 Computational methods for pure systems with two check characters

7.1 Computation

The computation of the check characters for these systems proceeds precisely as in the systems with one check character until the final stage, where an additional step is required in systems with a radix other than 10 to extract the two character values for the check characters. (For the check character system ISO 7064, MOD 97-10, see 7.4.) This is done by dividing the result by the radix. The integer quotient is the check character value for the position $i = 2$ and the remainder is the check character value for the position $i = 1$.

7.2 Example using recursive method

To compute the two check characters for the string "ISO 79" with the system ISO 7064, MOD 1271-36, using the recursive method and the alphanumeric character values given in table 3, the following steps are taken :

Step	Product brought forward	+	Next character value	=	Intermediate sum	Intermediate sum	×	Radix	=	Product	Product (mod 1271) carried forward
j	P_j	+	$a_{(n-j+1)}$	=	S_j	S_j	×	r	=	$P_{(j+1)}$	$P_{(j+1)}$ (mod M)
1	0	+	18	=	18	18	×	36	=	648	648
2	648	+	28	=	676	676	×	36	=	24336	187
3	187	+	24	=	211	211	×	36	=	7596	1241
4	1241	+	7	=	1248	1248	×	36	=	44928	443
5	443	+	9	=	452	452	×	36	=	16272	1020
6	1020	+	0†	=	1020	1020	×	36	=	36720	1132

† Since the position to be occupied by the first check character is still empty at this stage, its value is zero.

Step 7 : to calculate the check value, subtract the last $P_{(j+1)}$ (mod M) from (M + 1). Thus :

1271 + 1 = 1272

Then 1272 − 1132 = 140

To get the individual character values that make up 140 divide by the radix 36; this yields a quotient of 3 and an integer remainder of 32.

The quotient 3 is the value of the check character in position ($i = 2$) and the integer remainder 32 is the value of the check character in position ($i = 1$). Using the character values in table 3, these correspond to the characters 3 and W, so the full protected string is ISO 79 3W.

To check this string, steps 1 to 5 are carried out precisely as shown above, but steps 6 and 7 are as follows.

6	1020 + 3 = 1023	1023 × 36 = 36828	1240 (mod 1271)
7	1240 + 32 = 1272	(see note)	

1272 ≡ 1 (mod 1271), thus satisfying the check.

NOTE — The last character value is just added in and the sum is not multiplied by the radix.

7.3 Example using polynomial method

The procedure for computing the two check characters for the example in 7.2, the string ISO 79, by the polynomial method using the weights from table 4 and the character values from table 3 is as follows :

Character position i :	7	6	5	4	3	2	1
Weights W_i :	373	893	625	900	25	36	1
Character value a_i :	18	28	24	7	9		
Products :	6714	25004	15000	6300	225		

Sum : 6714 + 25004 + 15000 + 6300 + 225 = 53243 = 1132 (mod 1271)

The procedure described in step 7 of 7.2 is then followed, giving ISO 79 3W.