ICS 35.040
L 71

中华人民共和国国家标准

GB/T 17710—2008/ISO/IEC 7064:2003
代替 GB/T 17710—1999

信息技术　安全技术
校验字符系统

Information technology—Security technique—Check character systems

(ISO/IEC 7064:2003,IDT)

2008-07-16 发布　　2008-12-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前言 …… Ⅰ
引言 …… Ⅱ
1　范围 …… 1
2　术语和定义 …… 1
3　符号及其注释 …… 2
4　系统类型 …… 2
5　依从性及其冠名 …… 3
6　纯系统的说明 …… 4
7　带一位校验字符的纯系统的计算方法 …… 5
8　带两位校验字符的纯系统的计算方法 …… 7
9　混合系统说明 …… 9
10　混合系数的计算方法 …… 9
附录A（资料性附录）　对各种应用选择校验字符系统的准则 …… 11
附录B（资料性附录）　非拉丁字母的校验字符系统 …… 13
参考文献 …… 14

前　言

本标准等同采用 ISO/IEC 7064:2003《信息技术　安全技术　校验字符系统》，仅有编辑性修改。本标准代替 GB/T 17710—1999。本标准与 GB/T 17710—1999 的区别如下：

——标准的编排结构进行了调整；

——对 2.1、2.2、2.3、2.6 的术语定义进行了修改。

本标准中的附录 A 和附录 B 是资料性附录。

本标准由中华人民共和国工业和信息化部提出。

本标准由全国信息技术标准化技术委员会归口。

本标准起草单位：中国电子技术标准化研究所、中国标准化研究院。

本标准主要起草人：陈星、杨建军、黄家英、史立武、张明天。

本标准所代替标准的历次版本发布情况为：

——GB/T 17710—1999。

引　言

校验字符系统标准化的需求出于如下考虑：

a) 由于大量正在使用的系统中，许多系统具有相似的特征，而特征的许多的变化没有起到有效的作用；

b) 现有的系统几乎没有经过严格的数学验证，有些还存在严重的缺陷；

c) 系统的多样性削弱了校验字符系统的经济利益，而且经常妨碍对交换数据的校验。

因此，应选择一套小型兼容性系统，有效地满足各种应用的需要。该系统应经过验证，在各种应用的限制之内，高效地防止典型的复制和键入错误。

ISO 2180、ISO 2894(ISO 2894 已撤销)和 ISO 6166 也规定了校验字符系统，但它们只适用于特殊的领域，因此现有的系统无论如何不能获得本标准所规定的差错检测率。

附录 A 概述了为特定的应用而选用某一按本标准规定的校验字符系统时应考虑的准则。

附录 B 举例说明了在某些字母表数目超过 26 个字母的国家应用本标准的方法。

信息技术　安全技术
校验字符系统

1　范围

1.1　本标准规定了一组校验字符系统，它可以防止在复制或键入数据时产生的串的错误。串的长度可以是固定的或是可变的，包括以下字符集中的字符：

a)　数字（10个数字：0～9）；

b)　字母（26个字母：A～Z）；

c)　字母数字（字母和数字）。

串中嵌入的空格和特殊字符忽略不计。

1.2　本标准为生成校验字符和校验串产品规约了一致性要求，这些产品采用了本标准所给出的系统。

1.3　这些校验字符系统能检查出下列错误：

a)　所有的单一字符替换错误（即，单个字符被另一个字符所替换，如1234被错录为4234）；

b)　所有的或几乎所有的单一字符对换位置错误（即，相邻两个字符或隔一个字符的两个单一字符的位置互换，如12345被错录为123 54或12 54 3）；

c)　所有或几乎所有的循环移位错误（即，整个串被向左或向右循环移位）；

d)　大部分的双替换错误（即，在同一串中，分开的两处单一字符替换错误，如1234567被错录为72345 87）；

e)　大部分的其他错误。

1.4　本标准不包括专门为下列目的而设计的系统：

a)　既允许差错检测，又允许自动校正；

b)　检测故意误用；

c)　仅校验在机器之间交换的串。

1.5　本标准用于各组织之间的信息交换，极力推荐用于内部信息系统。

2　术语和定义

下列术语和定义适用于本标准。

2.1

校验字符　check character

可通过该串的数学关系来验证串的正确性所使用的附加字符。

2.2

校验字符系统　check character system

产生校验字符的和校验包含校验字符的串的一组规则。

2.3

补充校验字符　supplementary check character

不属于被保护串的字符集的校验字符。

2.4

模数　modulus

一个整数，它用作整除计算的除数以得到一个整数余数。

2.5

同余 congruence

一组整数的特性，彼此之差是模数的倍数。同余用符号“≡”表示。例如 39≡6(mod 11)，表示 39 和 6 相对于模数 11 是同余的，即 39－6＝33，33 是 11 的倍数。

2.6

基数 radix

几何级数的底。

3 符号及其注释

在本标准中使用了下列符号及其注释

a_i	位置 i 中的字符数字值。
i	字符位置的索引。
M	模数。
n	串中的字符个数，包括校验字符。
P_i, S_i, V	在校验字符计算时，用来存储中间结果的几个整数。
r	基数。
w_j	多项式法的权。
X, *	补充校验字符。
$:=$	表示在校验字符的过程规范中所使用的计算“置为等于”的符号，该计算符号指示应使该符号左边的整数值等于该符号右边的表达式的值。
$\equiv$	表示“同余”(见 2.5)的符号。
$\|\|_M$	表示 1 和 M 之间唯一整数的符号，该符号表示除以 M 后的余数；如果该余数是零，则值 M 应被替换。
$\|_{M+1}$	表示 0 和 M 之间唯一整数的符号，该符号表示除以(M+1)后的余数；在该计算之后，此余数决不是零。
(mod M)	表示 0 和 M－1 之间唯一整数的符号，该符号表示除以 M 后的余数。

4 系统类型

本标准规定了两类系统：

a) 纯系统(见第 6 章、第 7 章和第 8 章)；

b) 混合系统(见第 9 章、第 10 章)。

4.1 纯系统

表 1 中列出了纯系统并且在第 6 章、第 7 章和第 8 章中作了规定，每个系统的所有计算阶段都使用单一模数。

表 1 纯系统

校验字符系统冠名[a]	应用	校验字符数目及类型[b]
ISO/IEC 7064, MOD 11-2	数字串	1 个数字或补充校验字符 X
ISO/IEC 7064, MOD 37-2	字母数字串	1 个数字或字母或补充校验字符*
ISO/IEC 7064, MOD 97-10	数字串	2 个数字

表 1（续）

校验字符系统冠名[a]	应用	校验字符数目及类型[b]
ISO/IEC 7064,MOD 661-26	字母串	2 个字母
ISO/IEC 7064,MOD 1271-36	字母数字串	2 个数字或字母

[a] 在名称中，紧跟“MOD”之后的第一个数字是模数，第二个数字是基数。

[b] 前两个系统可以产生一个补充校验字符，但被校验串的字符集除外。（即，ISO/IEC 7064，MOD 11-2 的校验字符是 0～9 加上 X，ISO/IEC 7064，MOD 37-2 的校验字符是 0～9 和 A～Z 加上 *）。若补充校验字符不可用，则要求单个校验字符，就有可能避免发布产生补充校验字符的那些串；若既不能容忍补充校验字符，又不能避免产生校验字符的串，则应使用混合系统。

4.2 混合系统

表 2 和第 9 章、第 10 章中列出了混合系统。混合系统在计算中采用了两个模数，其中一个模数等于被保护的字符集中的字符数，另一个模数比它大 1，被保护串的字符集总是提供校验字符。

表 2 混合系统

校验字符系统冠名[a]	应用	校验字符数目及类型
ISO/IEC 7064,MOD 11,10	数字串	1 个数字
ISO/IEC 7064,MOD 27,26	字母串	1 个字母
ISO/IEC 7064,MOD 37,36	字母数字串	1 个数字或字母

[a] 在系统名称中，紧跟在 MOD 后面的两个数字是两个模数。

5 依从性及其冠名

5.1 串

在本标准中为相关应用而规定的系统之一所保护的串符合本标准。

5.2 生成校验字符的产品

5.2.1 依据本标准生成的校验字符产品（用软件或硬件实现）若没有其他限定，则应能生成本标准中的全部系统的校验字符。

5.2.2 不生成本标准中全部系统校验字符的产品，则应指明这些产品覆盖的那些系统。例如“按照 ISO/IEC 7064,MOD 11-2 生成校验字符”。

5.3 校验产品

5.3.1 按照本标准（无进一步限定），可校验本标准所生成的校验字符的产品（用软件或硬件实现），应能使用本标准的所有系统。

5.3.2 校验仅使用本标准中某些系统的串的产品描述，应说明该产品覆盖的那些系统。例如“校验使用 ISO/IEC 7064，MOD 11-2 的串”。

5.4 系统名称

5.4.1 通常应该使用表 1 和表 2 中给出的每一系统的全称，例如“ISO/IEC 7064 ,MOD 11-2”。

注：采用缩写形式“MOD 11”将会与使用模数 11 类似系统混淆。

5.4.2 当需要简化时，例如，数据元传输时往往需要同时标明用来保护该数据元的系统，可采用表 3 中的单一数字名称。

表 3 单一数字名称

校验字符系统	名 称
ISO/IEC 7064,MOD 11-2	1
ISO/IEC 7064,MOD 37-2	2
ISO/IEC 7064,MOD 97-10	3
ISO/IEC 7064,MOD 661-26	4
ISO/IEC 7064,MOD 1271-36	5
ISO/IEC 7064,MOD 11,10	6
ISO/IEC 7064,MOD 27,26	7
ISO/IEC 7064,MOD 37,36	8
无校验字符或非标准系统	0

6 纯系统的说明

6.1 公式

当下列公式成立时,串满足该校验:

$$\sum_{i=1}^{n} a^i \cdot r^{i-1} \equiv 1 (\mathrm{mod}\ M)$$

式中:

n——包括校验字符的串的字符个数;

i——表示从右边开始的字符所在位置索引(即,最右边的字符,$i=1$),空格与分割符不包括在内;

a_i——由表 4 规定的处于 i 位置上的字符值;

r——基数(即几何级数的底);

M——模数。

表 4 字符对应的值

字符	系统中数字串值	系统中字母串的值	系统中字母数字串的值
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
X[a]	10		
A		0	10
B		1	11
C		2	12
D		3	13
E		4	14

表 4（续）

字符	系统中数字串值	系统中字母串的值	系统中字母数字串的值
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
* [b]			36

[a] 为 ISO/IEC 7064 MOD 11-2。

[b] 为 ISO/IEC 7064 MOD 37-2。

6.2 计算

任何计算均按公式进行。

6.3 校验字符的位置

校验字符应设置在串的最右端。

7 带一位校验字符的纯系统的计算方法

纯系统有两种基本的计算方法：纯系统递归法和纯系统多项式法，两种方法的结果一致，并要求相同的乘量和加量。多项式系统要求更多的存储空间用来存储系统的权。

7.1 纯系统递归法

7.1.1 计算

在递归法中，串的字符从左到右逐个处理。下面将介绍生成校验字符 a_1 的计算规则。用 $j=1,\cdots,(n-1)$ 来表示索引。n 为包括校验字符在内的串中字符的数目。当 $j=1$ 时，定义 $P_j=0$。计算：

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

$$P_{j+1} := S_j \cdot r$$

式中：

a_{n-j+1} 为字符值，r 为基数。

选择下一个 a_1 时，下列公式应成立：

$$P_n + a_1 \equiv 1 (\mathrm{mod}\ M)$$

或

$$a_1 := (1 - P_n) (\mathrm{mod}\ M)$$

验证校验字符 a_1 的算法可以描述如下：在索引 $j=1,\cdots,n$ 时，其中，n 是在串中的字符数，包括校验字符，并且在 $j=1$ 时，定义 $P_j=0$。计算：

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

$$P_{j+1} := S_j \cdot r$$

如果下列公式成立，则假定该串是正确的，

$$S_n \equiv 1 (\mathrm{mod}\ M)$$

另一种办法是，生成校验字符 a_1 的过程可以进行重复。如果生成的校验字符相当于现有字符 a_1 则假定该串是正确的。

7.1.2 举例

假设使用校验字符系统 ISO/IEC 7064，MOD 11-2 为串“0794”提供一个校验字符。此时 $M=11$，$r=2$，$n=5$(4 个字符加 1 个校验字符)。按表 5 列出的步骤进行计算：

表 5 纯递归法实例

步骤	乘积	+	下一个字符值 (见 7.1.2 的注 1)	=	中间和	中间和	×	基数	=	作为下次计算值的乘积 (见 7.1.2 的注 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+校验字符值与 1(mod 11)是同余的。									

在这个例子中，P_n 的最终结果为 100，加上校验字符的值必须与 1(mod 11)同余，当 100 本身就与 1(mod 11)同余时，校验字符值必须为零，当校验字符加在串的最右边时，整个受保护的串是“0794 0”。

为了校验该串是否正确，如上所示，再按上述步骤 $j=1\sim5$ 进行计算，在计算中要包括校验字符值 0。如果该结果与 1(模 11)同余，则接受的串是有效的。

注 1：如果计算过程中任一步的结果 P_{j+1} 或者中间和 S_j 大于模数 M，则可减去模数的倍数，用其整余数继续计算。

在表 5 中：

$P_3=14$ 可处理为 $14-11=3$

$S_3=23$ 可处理为 $23-22=1$

$P_4=46$ 可处理为 $46-44=2$

注 2：在 ISO/IEC 7064，MOD 11-2 系统中有效的校验字符值是 0～10。如果校验字符的值为 10，就由附加校验字符“X”表示。如果原串是“079”这样的短串，在第三步计算结束时计算值为 46：

$$46 \equiv 2 (\text{模 } 11);$$

由于 2+10≡1(模 11)，因此完整串为“079 X”。

对该串进行校验时，第三步计算之后得到 46+10=56，与 1(模 11)同余，满足校验。

7.2 纯系统多项式法

7.2.1 计算

纯系统多项式法采用 r^{i-1} 或 r^{i-1}(模 M)的值乘以串中每一字符值来计算，用权 w_i 来表示。表 6 中列出了纯系统的 r^{i-1}(模 M)的前 15 个值。

将字符值与它们的权相乘，再将结果相加，如果这些结果之和与 1(模 M)同余，则包含校验字符在

内的串是有效的。

表 6 纯系统的权

位置索引	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
ISO/IEC 7064,MOD 11-2	5	8	4	2	1	6	3	7	9	10	5	8	4	2	1
ISO/IEC 7064,MOD 37-2	30	15	26	13	25	31	34	17	27	32	16	8	4	2	1
ISO/IEC 7064,MOD 97-10	53	15	50	5	49	34	81	76	27	90	9	30	3	10	1
ISO/IEC 7064,MOD 661-26	129	488	273	341	547	199	389	498	70	562	255	390	15	26	1
ISO/IEC 7064,MOD 1271-36	769	904	590	87	532	156	428	718	373	893	625	900	25	36	1

注：此处仅列出前 15 个位置的权，其余的可用公式 $w_i = r^{i-1} (\mathrm{mod}\ M)$ 无限扩展，w_i 为位置索引 i 的权。

7.2.2 举例

用多项式法产生校验字符的计算过程如下，仍以 7.1.2 中的串“0794”为例：

字符位置 i：	5		4		3		2	1	
权 $2^{i-1} (\mathrm{mod}\ 11)$：	5		8		4		2	1	
字符数 a_i：	0		7		9		4		
乘积：	0		56		36		8		
乘积的和：	0	+	56	+	36	+	8	=100	

总和 100 加上校验字符必须与 1(模 11 同余)，由于 100 本身与 1(模 11)同余，所以校验字符必定是零，这样整个串为“0794 0”。校验字符设置在串的右端。

用这种办法来校验串，需要与字符位置相关的权乘以字符值(包括校验字符在内)，结果相加，总和被 11 除，如果余数是 1，则通过验证。

校验整个串的计算如下：

字符位置 i：	5		4		3		2		1	
权 $2^{i-1} (\mathrm{mod}\ 11)$：	5		8		4		2		1	
字符数 a_i：	0		7		9		4		0	
乘积：	0		56		36		8		0	
乘积的和：	0	+	56	+	36	+	8	+	0	=100
										≡1(模 11)

满足验证要求。

注：最右边的位置，即 $r^0 = 1$ 的位置，是留给校验字符的位置，原串(不含校验字符)的最右端位置就是与 r 的权有关，此处为 2。

8 带两位校验字符的纯系统的计算方法

8.1 计算

这些系统与含一位校验字符的系统计算方法完全一致，只需再加一步，除了基数是 10 的系统求出两个字符值作为校验字符（对于校验字符系统 ISO/IEC 7064，MOD 97-10，见 8.4)，用 V 表示最后一步的计算结果。两位校验字符值可以用基数 r 除计算结果 V，得到的整商数即为 $i=2$ 位置上的校验字符值，余数则是 $i=1$ 位置上的校验字符值，或：

$$a_1 := V (\mathrm{mod}\ r)$$

$$a_2 := (V - a_1)/r$$

8.2 递归法应用举例

下面是用递归法，用 ISO/IEC 7064，MOD 1271-36 系统计算串“ISO 79”两个校验字符的例子，字母数

字字符值在表 4 中给出，表 7 中给出了第 1 步～第 6 步。在 1.1 中已说明串中嵌入的空格忽略不计。

表 7　带两位校验字符的纯递归法实例

步骤 j	乘积 P_j	+	下一个字符值 a_{n-j+1}	=	中间和 S_j	中间和 S_j	×	基数 r	=	计算结果 P_j+1	作为下次计算值的乘积(mod 1 271) $P_j+1(\text{mod } M)$
1	0	+	18	=	18	18	×	36	=	648	648
2	648	+	28	=	676	676	×	36	=	24 336	187
3	187	+	24	=	211	211	×	36	=	7 596	1 241
4	1 241	+	7	=	1 248	1 248	×	36	=	44 928	443
5	443	+	9	=	452	452	×	36	=	16 272	1 020
6	1 020	+	0[a]	=	1 020	1 020	×	36	=	36 720	1 132

[a] 被第一个校验字符占据的这一位置在这一步时仍是空的，所以其值为零。

最后一步(第 7 步)是计算校验字符值：用$(M+1)$减去最后的 $P_{j+1}(\text{mod } M)$，即：

$$1\ 271+1=1\ 272$$

然后

$$1\ 272-1\ 132=140$$

为得到单个的校验字符值，用 $V=140$ 除以基数 36，得到商数为 3，整余数为 32。

这样，商数 3 即为位置 $i=2$ 处的校验字符值，整余数 32 为位置 $i=1$ 处的校验字符值。按照表 4，3 与 32 分别对应着字符 3 和字符 W，因而带有校验字符的完整的串为："ISO 79 3W"。

需验证该串时，第 1 步～第 5 步如上所示，第 6 步，第 7 步如表 8 所示：

表 8　带两个校验字符的纯递归系统的实例验证

6 7	1 020+3=1 023 1 240+32=1 272	1 023×36=36 828 (见注)	1 240(mod 1 271)
1 272≡1(mod 1 271)，满足校验。 注：最后这个字符是刚加上的，因而该总数不再乘以基数。			

8.3　多项式应用举例

用多项式方法计算 7.2 中的串"ISO 79"的两个校验字符，其权采用表 6 中的值，字符值参照表 4，如表 9 所示。然后按照 8.2 中的第 7 步计算，得到"ISO 79 3W"。

表 9　带两位校验字符的多项式法实例

字符位置 i：	7	6	5	4	3	2	1
权 w_i：	373	893	625	900	25	36	1
字符值 a_i：	18	28	24	7	9		
乘积：	6 714	25 004	15 000	6 300	225		
乘积的和：	6 714 +	25 004 +	15 000 +	6 300 +	225	=53 243	
						=1 132(mod 1 271)	

8.4　ISO/IEC 7064，MOD 97-10 的简化规程

对该系统可遵守 8.2 和 8.3 中所述的规程。

但是，由于通常在十进制计数法中，该数字已经用基数为 10 的幂进行加权。可采用简化过程如下：在串后面添写两个 0，并除以 97，再用 98 减去上述余数，所得结果中的两个数字就是校验字符。

例如，对于串"794"，计算过程如下：

第一步:在校验字符位置上加两个 0:794 00;

第二步:除以 97,得商 818,整余数为 54;

第三步:计算校验字符值,(97+1)−54=44,将 44 加到原串后面,得 794 44。

为了验证,用 97 除该串,如果余数为 1,则满足要求。

9 混合系统说明

9.1 公式

在混合系统中,字符 M 在字符集中的位数为偶数。一个包括按标准混合公式产生的校验字符的串须满足下式的验证:

$$(\Lambda((((M+a_n)\|_M \cdot 2)\|_{(M+1)}+a_{(n-1)})_M \cdot 2)\|_{(M+1)}+\Lambda+a_1)\|_M=1$$

式中:

n——包括校验字符的串的字符数目;

i——从右侧计算的字符所在位置的符号(如最右端字符 $i=1$),空格和分割符不计;

a_i——表 4 中所列的 i 位置上的字符值;

M 和 $(M+1)$——两个模数,M 的数值等于该字符集中的字符数目;

$\|_M$——除以 M 后的整余数,如果为 0,则 M 值应被替换;

$|_{M+1}$——除以 $(M+1)$ 后的余数,在经过上述处理后余数绝对不会为 0。

9.2 校验字符的位置

校验字符设置在串的最右端。

10 混合系数的计算方法

这里仅给出了混合系统产生校验字符和验证含校验字符的串的基本方法,即混合系统递归法。

特别值得注意的是:与纯系统多项式法类似的计算方法在混合系统中不能得出相同的结果,因此不能采用。

10.1 混合系统递归法

10.1.1 计算

在递归法中,字符从左到右依次校验。

生成校验字符 a_1 的计算法则的描述为:用 $j=1\cdots(n-1)$,n 为包含校验字符在内的串中字符的数目。当 $j=1$ 时,定义 $P_j=M$,公式如下:

$$S_j := P_j|_{M+1}+a_{n-j+1}$$

$$P_{j-1} := S_j\|_M \cdot 2$$

式中:

$\|_M$——除以 M 后的整余数,如果为 0,则 M 值应被替换;

$|_{M+1}$——除以 $(M+1)$ 后的整余数,在经过上述处理后该余数不会为 0;

a_{n-j+1}——字符值。

所以下一个 a_1:

$$P_n+a_1 \equiv 1(\text{mod } M) \text{ 或 } a_1 := -(1-P_n)(\text{mod } M)$$

验证校验字符 a_1 的算法则描述为:用 $j=1,\cdots\cdots,(n-1)$,n 为包含校验字符在内的串中字符的数目。当 $j=1$ 时,定义 $P_j=0$。公式如下:

$$S_j := P_j|_{M+1}+a_{n-j+1}$$

$$P_{j+1} := S_j\|_M \cdot 2$$

如果 $S_n \equiv 1(\text{mod } M)$ 则串正确。

也就是说,生成校验字符 a_1 的过程可以重复。如果生成的校验字符和现有的字符 a_1 一致,则串

正确。

10.1.2 举例

假定用系统 ISO/IEC 7064,MOD 11,10 为串 0794 设置校验字符,其中 $M=10$,$M+1=11$,$n=5$(4 位字符加一位校验字符)。

计算结果列于表 10。

因此,校验字符的值为 5,完整的串为 0794 5,校验字符附加到原串的右端。

校验串的计算如表 10 第一步至第五步所示,且校验字符值 5 的计算也包括在内。最后结果必须与 1(mod 10)同余。

表 10 混合系统递归法实例

步骤 j	乘积	+	下一字符值	=	中间和	调整中间和	×	2	=	结果	调整后下次计算值的乘积
	P_j	+	a_{n-j+1}	=	S_j	$S_i \parallel_{10}$	×	2	=	P_{j+1}	$P_{j+1} \mid_{11}$
1	10	+	0	=	10	10	×	2	=	20	9
2	9	+	7	=	16	6	×	2	=	12	1
3	1	+	9	=	10	10	×	2	=	20	9
4	9	+	4	=	13	3	×	2	=	6	6
5	6	+校验字符值应与 1(mod 10)同余									

附 录 A
（资料性附录）
对各种应用选择校验字符系统的准则

系统的选择准则如表 11 所示，它包括：

a) 受保护的串的字符集（见第 2 列）；

b) 校验字符的字符集（第 3 列）。除了 ISO 7964，MOD 11-2，ISO 7064，MOD 37-2 以外，所有其他系统的校验字符集均与受保护的串的字符集是一样的。而这两个系统或者需要一个补充校验字符，或者需要不宜使用产生的补充校验字符的校验字符的串；

c) 校验字符位数（第 4 列）。除了两位校验字符的可接受性（根据费用和其他约束条件）必须与系统需要的校验字符所提供的有力保护所协调出的益处相权衡；

d) 未被检出的错误百分比（第 5 列），即可能检查不出来的各种类型错误的百分比。这些错误有下述几种类型：

1. 单替换错误——一个单一字符被另一个单一字符替换；
2. 单一对换错误——单个字符的对换，相邻的（$d=1$）两个字符或相隔一个字符的（$d=2$）两个字符之间的互换错误；
3. 双替换错误——在同一个串中，两个分隔的单一字符的替换错误；
4. 循环位移——串向左或向右的循环位移（表中所列的错误率仅指中等距离（$d<10$）的循环位移错误）；
5. 其他错误——所有上述未指出的错误；
6. 残余差错（第 6 列）。

残余差错给出了每 100 000 个差错中未被检测到的各种差错类型的典型范围。

表 A.1 中较低数字是指有利的混合差错类型的典型最佳情况，较高数字是指不利的混合差错类型的典型最差情况（例如，上述差错类型平均出现率并不总能被检测到）。这些数字仅当严格的统计不可用时，用作指导。实践中应考虑可能出现偏差。其数值是基于下面错误出现率的范围给出的：

单替换	60% ～ 85%
单对换，$d=1$	5% ～ 15%
单对换，$d=2$	1% ～ 2%
双替换	5% ～ 15%
位移	0% ～ 5%
其他	1% ～ 10%

未被检出的错误百分比反应了校验字符系统孤立使用的情况。如果把这些系统与其他校验结合起来使用，效果会更好。其他校验包含一致性校验、字符类型与串长度校验等等，例如，一个串长度校验就会检查出字符的所有删改或插入错误。

表 A.1 系统的选择准则

1	2	3	4	5						6
校验字符系统 ISO 7064 MOD	受保护串的字符集	校验字符的字符集	校验字符的位数	未被检测到的差错的百分比						剩余差错（每 100 000 个错误中）
				单替换	单换位		双替换	位移 $d<10$	其他	
					$d=1$	$d=2$				
11-2	数字	数字加上“X”[a]	1	0.0	0.0	0.0	10.0	0.0	9.1	600～2 400

表 A.1（续）

1	2	3	4	5						6
校验字符系统 ISO 7064 MOD	受保护串的字符集	校验字符的字符集	校验字符的位数	未被检测到的差错的百分比						剩余差错（每 100 000 个错误中）
				单替换	单换位		双替换	位移 $d<10$	其他	
					$d=1$	$d=2$				
11,10	数字	数字	1	0.0	2.2	9.3	11.0	0.0	10.0	760～3 100
97-10	数字	数字	2	0.0	0.0	0.0	1.0	0.0	1.0	20～250
27,26	字母	字母	1	0.0	0.31	2.4	4.0	0.0	3.8	250～1 100
661-26	字母	字母	2	0.0	0.0	0.0	0.1	0.0	0.15	6～30
37-2	字母数字	字母数字加上“*”[b]	1	0.0	0.0	0.0	2.7	0.0	2.7	160～700
37,36	字母数字	字母数字	1	0.0	0.16	1.7	2.8	0.0	2.8	180～740
1 271-36	字母数字	字母数字	2	0.0	0.0	0.0	0.04	0.0	0.08	3～15

[a] 可通过不使用产生 10 作为校验字符值的串来避免补充校验字符。

[b] 可通过不使用产生 36 作为校验字符值的串来避免补充校验字符。

附 录 B
（资料性附录）
非拉丁字母的校验字符系统

本附录将举例说明如何将此系统扩展而满足那些不仅使用 26 个拉丁字母的国家的需求。

下面以丹麦的 29 个字母为例(A～Z、Å Æ Ø)。

由于 29 是个质数，并由于 2 具有 $2^a \equiv 1 \pmod{29}$ 就是 28 (=29−1)的最小正整数的特性，所以，当 29 作为模数、2 作为基数时，可以使用纯系统。仅在下列元素方面，这可能不同于 ISO 系统。

名称：(Danish) MOD 29-2

表 4：增加了字母系统的字符值：

Æ：26

Ø：27

Å：28

表 6：增加了表 B.1 中的 MOD 29-2 的权。

表 B.1 (Danish) MOD 29-2 的纯系统权

位置下标	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
(Danish) MOD 29-2	28	14	7	18	9	19	24	12	6	3	16	8	4	2	1

参 考 文 献

[1] GB/T 5795—2006 中国标准书号(ISO 2108:2005,MOD).

[2] GB/T 21076—2007 证券及相关金融工具 国际证券识别编字符体系(ISO 6166:2001,MOD).

[3] ISO 2894:1980 凸印式信用卡 规范 编号系统和注册规程.

中 华 人 民 共 和 国
国 家 标 准
信息技术 安全技术
校验字符系统
GB/T 17710—2008/ISO/IEC 7064:2003
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.25 字数 29 千字
2008年11月第一版 2008年11月第一次印刷
*
书号:155066·1-34939

GB/T 17710—2008/ISO/IEC 7064:2003

GB/T 17710-2008

打印日期:2010年11月8日 F010