



中华人民共和国国家标准

GB/T 17710—1999
idt ISO 7064:1983

数据处理 校验码系统

Data processing—Check character systems



1999-03-23 发布



C200005989

1999-10-01 实施

国家质量技术监督局 发布

前言

本标准等同采用国际标准 ISO 7064:1983(1996 年经 ISO/IEC JTC1 SC14 确认)。

本标准提供了对键入和抄录数据时发生的错误进行校验的方法,目的是满足各系统之间对交换数据的校验。与其他存在的校验码系统相比,本标准规定的校验码系统可直接校验数字型、字母型和数字字母型字符串,操作方便;检错类型多,检错能力强;并经过了严格的数学验证,所使用的数学知识浅显,易于接受和推广。

本标准的内容包括前言、引言及应用范围、第一篇 总则、第二篇 纯系统、第三篇 混合系统和两个附录,附录 A 和附录 B 是标准的附录。

本标准由中国标准化与信息分类编码研究所提出。

本标准主要起草单位:中国标准化与信息分类编码研究所。

本标准的主要起草人:谢民、丘维声、丁雅娴、胡家璋、李小林。

本标准由全国信息技术标准化技术委员会数据元表示法分技术委员会归口并负责解释。

1 范围	1
2 规范性引用文件	2
3 术语和定义	3
4 总则	4
5 纯系统	5
6 混合系统	6
7 附录 A 校验码系统性能指标	7
8 附录 B 校验码系统性能指标	8

ISO 前言

ISO(国际标准化组织)是国际范围内各国标准组织(ISO 成员)的联盟,其工作的开展主要通过 ISO 技术委员会,对技术委员会工作感兴趣的每一成员,经授权后,可成为该技术委员会的成员。与 ISO 有联系的其他国际组织、政府或非政府组织,可参与 ISO 的工作。

技术委员会采纳的标准草案应提交全体成员组织讨论,通过后方可被 ISO 委员会接纳为国际标准。

国际标准 ISO 7064 由 ISO/TC97(ISO/IEC JTC1 前身)信息处理系统技术委员会制定,并在 1981 年 11 月提交成员组织讨论。

以下是通过此标准的成员组织:

比利时	联邦德国	南非共和国
中华人民共和国	爱尔兰	西班牙
捷克斯洛伐克	意大利	瑞典
丹麦	日本	瑞士
阿拉伯埃及共和国	荷兰	英国
芬兰	波兰	美国
法国	罗马尼亚	

全体成员组织一致同意通过本标准。

注:1996 年 8 月,ISO/IEC JTC1 SC14 组织 P 成员,对包括本标准在内的几个标龄较长的国际标准进行了阶段审核,各 P 成员组织均同意不需修订本标准,SC14 于 1996 年 12 月正式宣布 ISO 7064:1983 仍可继续使用。

目 次

前言 I

ISO 前言 II

0 引言 1

1 范围 1

第一篇 总 则

2 定义 2

3 类型 2

4 系统一致性和表示法 3

第二篇 纯 系 统

5 纯系统的说明 3

6 带一位校验码的纯系统的计算方法 5

7 带有两位校验码的纯系统的计算方法 7

第三篇 混 合 系 统

8 混合系统说明 8

9 混合系统的计算方法 8

附录 A(标准的附录) 校验码应用时系统的选择原则 10

附录 B(标准的附录) 非拉丁字母的校验码系统 11

中华人民共和国国家标准

数据处理 校验码系统

GB/T 17710—1999
idt ISO 7064:1983

Data processing—Check character systems

0 引言

目前,正在使用的校验码系统有一百多个,其中许多系统的特性非常近似,大多数系统并未起到有效的作用。现存的应用系统中,仅有少数经过严格的数学验证,有些还存在严重的缺陷。同时,系统的多样性无形中也损害着校验码系统的经济效益,常影响对交换数据的校验。因此,必须选择一些可满足不同需要的、兼容的校验码系统。本标准提供的校验码系统已经过数学验证,在其适用范围内,通过提供可靠的保护,可防止常见的抄录和键入错误。

ISO 2108、ISO 2984 和 ISO 6166 也规定了校验码系统,但它们只能用于专门的领域,其错误检测率低于本标准的规定。

附录 A 概述了为某一用途而选用本标准校验码系统时应考虑的准则。

附录 B 举例说明了当国家字母的数目与国际上通用的 26 个字母不同时,应如何建立兼容的本国校验码系统,并设计了具体的扩展方式。

1 范围

1.1 本标准规定的校验码系统,可以防止在抄录和键入字符串时产生的错误。字符串的长度或固定或可变,包括下列字符集中的字符:

- 1) 数字型 (10 个数字:0~9)
- 2) 字母型 (26 个字母:A~Z)
- 3) 字母数字型 (字母和数字)

字符串中嵌入的空格和特殊字符忽略不计。

1.2 对使用本标准产生校验码或校验字符串的产品,本标准规定了一致性要求。

1.3 本标准规定的校验码系统能检查出下列错误:

- 1) 所有的单一字符替代错误(即单个字符被另一字符所替换,如1234 被错录为4234);
- 2) 所有的或几乎所有的单一字符对换错误(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);
- 3) 所有的或几乎所有的位移错误(即整个字符串被向左或向右移位,如 123被录入为123);
- 4) 大部分的双替代错误(即在同一字符串中,分开的两处单一字符对换错误,如 1234567 被错录为 72345 87);
- 5) 大部分的其他错误。

1.4 本标准不适用于经特殊设计的专门系统,如:

- 1) 既能查错又能自动更正的系统;
- 2) 检查故意伪造的错误的系统;
- 3) 检查仅在计算机之间进行交换的字符串的系统。

1.5 本标准用于各组织之间的信息交换,也是内部信息系统信息交换的有力工具。

国家质量技术监督局 1999-03-23 批准

1999-10-01 实施

第一篇 总 则

2 定义

本标准采用下列定义：

2.1 校验码 checker character

可通过数学关系来验证代码正确性的附加字符。

2.2 校验码系统 checker character system

产生校验码并校验包括校验码在内的字符串的一套规则。

2.3 附加符,附加校验码 supplementary character

受保护的一系列字符串所构成的字符集以外的校验码。

2.4 模数 modulus

为使整除运算获得整数而用作除数的整数。

2.5 同余 congruence

指在一组整数中,两两之差与模数有倍数关系的特性。同余用符合“ $\equiv$ ”表示。如 $39 \equiv 6 \pmod{11}$,即指 $39 - 6 = 33$ 是 11 的倍数。

2.6 底数 radix

几何级数的基数。

3 类型

本标准规定了两类系统：

1) 纯系统；

2) 混合系统。

3.1 纯系统

表 1 中列出了纯系统(详见第二篇),每一个系统的所有运算都使用单一模数。

表 1 纯系统

校验码系统表示法 ¹⁾	适用范围	校验码数目及类型 ²⁾
ISO 7064 MOD 11-2	数字型字符串	1 位数字或附加符 X
ISO 7064 MOD 37-2	字母数字型字符串	1 位数字或字母或附加符 *
ISO 7064 MOD 97-10	数字型字符串	2 位数字
ISO 7064 MOD 661-26	字母型字符串	2 位字母
ISO 7064 MOD 1271-36	字母数字型字符串	2 位数字或字母
1) 在 MOD 之后的第 1 个数字是模数,第 2 个数字是底数。 2) 前两个系统可在被校验的字符串处产生一位附加校验码,(例如 ISO 7064 MOD 11-2 产生的校验码是 0~9 及 X,ISO 7064 MOD 37-2 的校验码是 0~9,A~Z 及 *)。当不能使用附加校验码,又只能有一位校验码时,应避免使用产生附加校验码的系统;如果既不能使用附加校验码,又不能使用一位校验码,则应使用混合系统。		

3.2 混合系统

表 2 中列出了混合系统(详见第三篇)。混合系统在运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,形成的校验码位于被保护的字符串组成的字符集内。

表 2 混合系统

校验码系统表示法 ¹⁾	应用	字符数目及类型
ISO 7064 MOD 11,10	数字串	1 位数字
ISO 7064 MOD 27,26	字母串	1 位字母
ISO 7064 MOD 37,36	字母数字串	1 位数字或字母

1) 在系统表示法中,紧跟在 MOD 后面的两个数字是两个模数。

4 系统一致性和表示法

4.1 字符串

本标准为不同的应用规定了不同的校验码系统,受这些系统保护的字符串应遵循本标准的规定。

4.2 生成校验码的产品

4.2.1 若无更严格的条件限制,可为本标准生成校验码的产品(软件或硬件),应能为本标准的所有系统生成校验码。

4.2.2 对不能使本标准的所有系统生成校验码的产品,应说明它们的特定使用范围。如“为 ISO 7064, MOD 11-2 生成的校验码”。

4.3 校验产品

4.3.1 若无更严格的条件限制,可校验本标准所生成的校验码的产品(软件或硬件),应能使用本标准的所有系统。

4.3.2 对仅能用本标准中某些校验码系统的产品,应说明它们所使用的系统。如“用 ISO 7064, MOD 11-2 生成的校验字符串”。

4.4 系统表示法

4.4.1 通常采用表 1 和表 2 中给出的每一系统的全称表示,例如“ISO 7064, MOD 11-2”。

注:采用缩写形式“MOD 11”将会与使用模数 11 的类似系统混淆。

4.4.2 当需要简化时,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,可采用下列单一数字表示法:

校验码系统	表示法	校验码系统	表示法
ISO 7064, MOD 11-2	1	ISO 7064, MOD 11,10	6
ISO 7064, MOD 37-2	2	ISO 7064, MOD 27,26	7
ISO 7064, MOD 97-10	3	ISO 7064, MOD 37,36	8
ISO 7064, MOD 661-26	4	无校验码或非标准系统	0
ISO 7064, MOD 1271-36	5		

第二篇 纯 系 统

5 纯系统的说明

5.1 公式

字符串应满足下列公式的校验:

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

公式中: n ——包括校验码的字符串的字符个数;

i ——表示从右边开始的字符所在位置序号(包括校验码在内),即最右边的字符 $i=1$,空格与分割符不计在内;

a_i ——由表 3 规定的处于 i 位置上的字符值；

r ——底数(即几何级数的基数)；

M ——模数。

表 3 字符对应的值

字符	系统中数字字符值	系统中字母字符值	系统中字母数字字符值
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
为 ISO 7064 MOD 11-2 设置的附加符 X	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

表 3 (完)

字符	系统中数字字符值	系统中字母字符值	系统中字母数字字符值
U		20	30
V		21	31
W		22	32
X		23	33
Y		24	34
Z		25	35
为 ISO 7064 MOD 37-2 设置的附加符 *			36

5.2 运算

任何运算均按公式进行。

5.3 校验码的位置

校验码设在字符串的最右端。

6 带一位校验码的纯系统的计算方法

纯系统有两种基本运算方法:纯系统递归法和纯系统多项式法,两种方法的结果一致。

6.1 递归法

6.1.1 运算

在递归法中,字符串的字符从左到右逐个处理。用 $j=1, \dots, n$ 来表示下标。 n 为包括校验码在内的字符串中字符的数目。当 $j=1$ 时,定义 $P_j=M$ 。

计算如下:

$$S_j = P_j + a_{(n-j+1)}$$
$$P_{(j+1)} = S_j \times r$$

其中, $a_{(n-j+1)}$ 为字符值, r 为底数。

如果 $S_n \equiv 1 \pmod{M}$, 则字符串满足校验要求。选择校验码 a_1 时, 应使之满足公式 $P_n + a_1 \equiv 1 \pmod{M}$ 。

6.1.2 举例

假定使用校验码系统 ISO 7064, MOD 11-2 为字符串 0794 设置一个校验码。此时 $M=11, r=2, n=5$ (4 位字符加 1 位校验码)。运算过程如下:

步骤 j	前次运 行结果 P_j	下一字 符值 $a_{(n-j+1)}$	中间 和 ¹⁾ $= S_j$	中间和 $\times$ 底数 $S_j \times r$	运算结果 ¹⁾ : $= P_{(j+1)}$
1	0	+	0	=	0
2	0	+	7	=	7
3	14	+	9	=	23
4	46	+	4	=	50
5	100+校验码值要与 1(mod 11)同余				

此处结果 P_n 为 100, 加上校验码的值必须与 1(mod 11)同余, 而 100 本身就和 1(mod 11)同余, 因此校验码值为零, 整个受保护的字符串则为 0794 0, 校验码加在字符串的最右边。

为了校验该字符串是否正确, 如上所示, 再按步骤 $j=1 \sim 5$ 进行计算, 将校验码值 0 也包括在内。如果运算结果与 1(模 11)同余, 则证明该字符串是正确的。

注

1. 如果计算过程中任一步的结果 $P_{(j+1)}$ 或中间和 S_j 大于模数 M , 则可减去模数的倍数, 用其整余数继续运算。如上例中:
- $P_3=14$ 可处理为 $14-11=3$
- $S_3=23$ 可处理为 $23-22=1$
- $P_4=46$ 可处理为 $46-44=2$
2. 在 ISO 7064, MOD11-2 系统中有效的校验码值是 0~10。如果校验码的值为 10, 就由字符“X”表示。如果原字符串是 079 这样的短字符串, 在第三步计算结束时运算值为 46, $46 \equiv 2 \pmod{11}$, 由于 $2+10 \equiv 1 \pmod{11}$, 因此带有校验码的完整字符串为 079 X。对该字符串进行检验时, 第三步运算之后得到 $46+10=56$, 与 1 (模 11) 同余, 满足校验。

6.2 多项式法

6.2.1 运算

纯系统多项式法采用 $r^{(i-1)}$ 或 $r^{(i-1)} \pmod{M}$ 的值乘以字符串中每一字符值来计算。表 4 中列出了所有纯系统的 $r^{(i-1)} \pmod{M}$ 前 15 个值。

将字符值与它们的权数相乘, 再将结果相加, 如果这些结果之和与 1 (模 M) 同余, 则包含校验码在内的字符串是有效的。

表 4 纯系统的权数

位置序号	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

注: 此处仅列出前 15 个位置的权数, 其余的可用下列公式无限扩展:

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

W_i 为位置序号 i 的权数

6.2.2 举例

用多项式法产生校验码的计算过程如下, 仍以 6.1.2 中的字符串 0794 为例:

字符位置 i	5	4	3	2	1
权数 $2^{(i-1)} \pmod{11}$	5	8	4	2	1
字符值 a_i	0	7	9	4	
乘积	0	56	36	8	
乘积的和	$0 + 56 + 36 + 8 = 100$				

总和 100 加上校验码必须与 1 (模 11) 同余, 由于 100 本身与 1 (模 11) 同余, 所以校验码必定为零, 这样整个字符串为 0794 0。校验码设置在字符串的最右端。

用这种方法来校验字符串, 需用与字符位置相关的权数乘以字符值 (包括校验码在内), 结果相加, 总和被 11 除, 如果余数是 1, 则通过验证。

字符位置 i	5	4	3	2	1
权数 $2^{(i-1)} \pmod{11}$	5	8	4	2	1
字符值 a_i	0	7	9	4	0
乘积	0	56	36	8	0
乘积的和	$0 + 56 + 36 + 8 + 0 = 100$				

$100 \equiv 1 \pmod{11}$

满足验证要求。

注：最右边的位置，即 $r^0=1$ 的位置，是留给校验码的位置。因此，原字符串（不含校验码）的最右端位置就与 r 的权数（ W_2 ）有关，此处 W_2 为2。

7 带两位校验码的纯系统的计算方法

7.1 运算

这些系统与含一位校验码的系统计算方法完全一致，只需再加一步，除了底数是10的系统求出两个字符值作为校验码（对于校验码系统 ISO 7064, MOD 97-10, 见 7.4）。用底数除运算结果得到的整商数即为 $i=2$ 位置上的校验码值，余数则是 $i=1$ 位置上的校验码值。

7.2 递归法应用举例

下面是采用递归法，用 ISO 7064, MOD 1271—36 系统计算字符串“ISO 79”两个校验码的例子，字母数字字符值在表 3 中给出。运算步骤如下：

步骤 j	前次运算结果 P_j	下一字符值 $a_{(n-j+1)}$	中间和 S_j	中间和 $\times$ 底数 $S_j \times r$	结果 $P_{(j+1)}$	作为下次运算值的结果(mod 1271) $P_{(j+1)} \pmod{M}$
1	0	18	18	$18 \times 36 = 648$	648	648
2	648	28	676	$676 \times 36 = 24\,336$	24 336	187
3	187	24	211	$211 \times 36 = 7\,596$	7 596	1 241
4	1 241	7	1 248	$1\,248 \times 36 = 44\,928$	44 928	443
5	443	9	452	$452 \times 36 = 16\,272$	16 272	1 020
6	1 020	0 ¹⁾	1 020	$1\,020 \times 36 = 36\,720$	36 720	1 132

1) 被第一个校验码占据的这一位置在这一步时仍是空的，所以其值为零。

第 7 步：为了计算校验码值，用 $(M+1)$ 减去最后的 $P_{(j+1)}$ 值：

$$1\,271+1=1\,272$$
$$1\,272-1\,132=140$$

为得到单个的校验字符值，用 140 除以底数 36，商数是 3，整余数为 32。

这样，商数 3 即为位置 $i=2$ 处的校验码值，整余数 32 为位置 $i=1$ 处的校验码值。按照表 3，3 与 32 分别对应着字符 3 和字符 W，因而带有校验码的完整的字符串为 ISO 79 3W。

需验证该字符串时，第 1~5 步如上所示，第 6, 7 步如下：

6	$1\,020+3=1\,023$	$1\,023 \times 36 = 36\,828$	$1\,240 \pmod{1\,271}$
7	$1\,240+32=1\,272$	(见注)	

$1\,272 \equiv 1 \pmod{1\,271}$ ，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底数。

7.3 多项式法应用举例

用多项式法计算 7.2 中的字符串 ISO 79 的两个校验码，其权数采用表 4 中的值，字符值参照表 3，步骤如下：

字符位置 i	7	6	5	4	3	2	1
权数 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	$6\,714+25\,004+15\,000+6\,300+225=53\,243=1\,132 \pmod{1\,271}$						

然后按照 7.2 中的第 7 步计算，得到 ISO 79 3W

7.4 ISO 7064, MOD 97-10 的简化程序

对该系统可采用 7.2 和 7.3 中所叙述的步骤。

通常,十进制中的数字已经乘以 10 的幂数,因此可采用简化步骤如下:在字符串后面添写两个 0,然后除以 97,再用 98 减去上述余数,所得结果中的两个数字就是校验码。

例如,对于字符串 794,计算过程如下:

第一步:在校验码位置上加两个 0:794 00

第二步:除以 97,得商 818,整余数为 54

第三步:计算校验码值, $(97+1)-54=44$,将 44 加到原字符串后面,得 794 44

为了验证,用 97 除该字符串,如果余数为 1,则满足要求。

第三篇 混合系统

8 混合系统说明

8.1 公式

一个包括按标准混合公式产生的校验码的字符串须满足下式的验证:

$$(\cdots(((M+a_n) \parallel_M \times 2) |_{(M+1)} + a_{(n-1)}) \parallel_M \times 2) |_{(M+1)} + \cdots + a_1) \parallel_M = 1$$

式中: n ——包括校验码的字符串的字符数目;

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

a_i ——表 3 中所列出的 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(此数总是偶数);

$\parallel_M$ ——除以 M 后的余数,如果其值为零,则用 M 代替;

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

8.2 校验码的位置

校验码设置在字符串的最右端。

9 混合系数的计算方法

这里仅给出了混合系统产生校验码和验证含校验码的字符串的基本方法,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。

9.1 递归法

9.1.1 运算

在递归法中,字符串的字符从左到右逐个处理。用 $j=1, \dots, n$ 来表示。 n 为包括校验码在内的字符串中字符的数目。当 $j=1$ 时,定义 $P_j=M$ 。公式如下:

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

$$P_{(j+1)} = S_j \parallel_M \times 2$$

式中: $\parallel_M$ ——除以 M 后的整余数,如果为 0,则用 M 代替;

$|_{(M+1)}$ ——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。

验证:如果 $S_n \equiv 1 \pmod{M}$,则字符串正确。确定校验码 a_1 时,应使之满足 $P_n + a_1 \equiv 1 \pmod{M}$ 。

9.1.2 举例

假定用系统 ISO 7064, MOD 11, 10 为字符串 0794 设置校验码,其中 $M=10$, $(M+1)=11$, $n=5$ (4 位字符加一位校验码)计算步骤如下:

步骤 j	前次运算结果 P_j	下一字符值 $+ a_{(n-j+1)}$	中间和 $= S_j$	调整中间和 $S_i \parallel_{10}$	$\times$	2	=	结果 $P_{(j+1)}$	调整后作为下次运算的结果 $P_{(j+1)} \mid_{11}$		
1	10	+	0	=	10	$\times$	2	=	20	9	
2	9	+	7	=	16	6	$\times$	2	=	12	1
3	1	+	9	=	10	10	$\times$	2	=	20	9
4	9	+	4	=	13	3	$\times$	2	=	6	6
5	6+校验码值应与 1(mod 10)同余										

由上式得到校验码值5,完整的字符串为07945,校验码放在原字符串的最右端。验证时,第一至五步如上所示,且校验码值5的计算也包括在内。最后结果必须与1(mod 10)同余。

位置	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100

附录 A
(标准的附录)

校验码应用时系统的选择原则

系统选择原则如表 A1 所示,包括下述内容:

- a) 受保护的字符串的字符集(见第二栏)。
- b) 校验码的字符集(第三栏)。除了 ISO 7064,MOD11-2 和 ISO 7064,MOD37-2 以外,所有其他系统的校验码集均与受保护的字符串的字符集是一样的。而这两个系统或者需要一个附加校验码,或者不使用产生附加符的校验码字符串。
- c) 校验码位数(第四栏)。两位校验码的可接受性(根据费用和其他限制条件)必须与因系统需要校验码而提供的有力保护所带来的益处相权衡。
- d) 未被检出的错误百分比(第五栏),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) 单替代错误——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) 双替代错误——在同一个字符串中,两个分隔的单一字符的替换错误;
- 4) 移位——字符串向左或向右的位移(表中所列的错误率仅指中等距离($d<10$)的位移错误);
- 5) 其他错误——所有上述未指出的错误。

- e) 剩余差错(第六栏)。剩余差错给出了每 100 000 个错误中未被查出的各种错误类型的典型范围。

表中较低的数值是适于各种错误类型交叉时特有的最好情况,较高的数值是错误类型交叉最差的情况。(例如,上述错误类型平均出现率并不总能被检出)。这些数字仅仅作为当确定的统计数字无法得到时的指导性数字,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:

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

未被检出的错误百分比反映了校验码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、字符类型与字符串长度校验等等,例如,一个字符串长度校验就会检查出字符的所有删改或插入错误。

表 A1 系统选择的原则(概要)

1	2	3	4	5						6	7
校验码系统 ISO 7064 MOD	受保护的 字符串的 字符集	校验码的 字符集	校验码 位数	未被检出的错误的百分比						剩余差错 (每 100 000 个错误中)	说明
				单替换	单对换		双替换	位移 $d=10$	其他		
					$d=1$	$d=2$					
11-2	数字	数字加 附加符 “X”	1	0	0	0	10	0	9.1	600~2 400	在字符串不生 成 校 验 码 10 时,可不使用附 加符
11,10	数字	数字	1	0	2.2	9.3	11	0	10	760~3 100	—
97-10	数字		2	0	0	0	1	0	1	20~250	—

表 A1 （完）

1	2	3	4	5						6	7
校验码系统 ISO 7064 MOD	受保护的 字符串的 字符集	校验码的 字符集	校验码 位数	未被检出的错误的百分比						剩余差错 (每 100 000 个错误中)	说明
				单替换	单对换		双替换	位移 $d=10$	其他		
					$d=1$	$d=2$					
27,26 661-26	字母 字母	字母 字母	1 2	0 0	0.31 0	2.4 0	4 0.1	0 0	3.8 0.15	250~1 100 6~30	— —
37-2	字母数字	字母数字 加附加符 “*”	1	0	0	0	2.7	0	2.7	160~700	在字符串不生成校验码 36 ¹⁾ 时,可不使用附加符
37,36 1271-36	字母数字 字母数字	字母数字 字母数字	1 2	0 0	0.16 0	1.7 0	2.8 0.04	0 0	2.8 0.08	180~740 3~15	— —

附 录 B

(标准的附录)

非拉丁字母的校验码系统

本附录将举例说明如何将此系统扩展而满足那些国家字母非 26 个的国家的需要使用。

下面以丹麦的 29 个字母为例(A~Z、Æ、Ø和 Å)。由于 29 是个质数,纯系统可用它作为模数。下面仅列出该系统与 ISO 系统的不同之处:

表示法:(丹麦) MOD 29-2

表 3:在字母系统中增加 3 个字符值:

Æ:26

Ø:27

Å:28

表 4:为 MOD 29-2 增加下列权数:

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

采用说明:

1) ISO 7064:1983 中,此数为 10,本标准经过推导,认为此数应为 36,ISO 7064 原文有误。

