ICS 35.100.60
L 79

中华人民共和国国家标准

GB/T 16263.1—2006/ISO/IEC 8825-1:2002
代替 GB/T 16263—1996

信息技术 ASN.1编码规则 第1部分:基本编码规则(BER)、正则编码规则(CER)和非典型编码规则(DER)规范

Information technology—ASN.1 encoding rules—Part 1:Specification Of Basic Encoding Rules(BER), Canonical Encoding Rules(CER) and Distinguished Encoding Rules(DER)

(ISO/IEC 8825-1:2002,IDT)

2006-03-14 发布　　2006-07-01 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

GB/T 16263 在《信息技术　ASN.1 编码规则》的总标题下，目前包括以下两个部分：

——第 1 部分(即 GB/T 16263.1)：基本编码规则(BER)、正则编码规则(CER)和非典型编码规则(DER)规范；

——第 2 部分(即 GB/T 16263.2)：紧缩编码规则(PER)规范。

本部分为 GB/T 16263 的第 1 部分，等同采用国际标准 ISO/IEC 8825-1:2002《信息技术　ASN.1 编码规则：基本编码规则(BER)、正则编码规则(CER)和非典型编码规则(DER)规范》(英文版)。与该项国际标准等同的文本是 ITU-T 建议 X.690。

本部分从实施之日起代替 GB/T 16263—1996《信息处理系统　开放系统互连　抽象语法记法一(ASN.1)基本编码规则规范》。与 GB/T 16263—1996 相比，本次修订在内容上作了如下变化：

——第 3 章"术语和定义"中，增加了"正则编码"、"尾 0 位"两个术语，将"构造编码"修订为"结构化编码"、"简单编码"修订为"原始编码"、"接收者"修订为"接受器"、"发送者"修订为"发送器"；

——第 4 章"缩略语"中，增加了"BER"、"CER"、"DER"和"ULA"四个缩略语。4.2 条"记法"修订为第 5 章。4.2.2 和 4.2.3 修订为第 6 章的第 6.1 和 6.2 条，增加了 6.3 条；

——将第 5 章修订为第 7 章，增加了 7.4 条；

——将第 6 章修订为第 8.1 条，增加第 8 章标题"基本编码规则"。图 1～图 4 中分别去掉外框；

——将第 7 章修订为第 8.2 条、第 8 章修订为第 8.3 条，……，第 18 章修订为第 8.13 条，去掉第 19 章，将第 20 章修订为第 8.14 条，去掉第 21 章，增加了 8.15～8.18 条，将第 22 章修订为 8.19 条、增加了第 8.20 条，将第 23 章修订为第 8.21 条并增加了 8.21.6～8.21.10 条，将表 2 修订为表 3，去掉第 24 章，增加了第 8.22 条～第 8.23 条，增加第 9 章～第 11 章，将第 25 章修订为第 12 章；

——修订附录 B 中的内容，补充了在本部分中赋值的值；

——所有示例中的英文尽量保留不译。

按照 GB/T 1.1—2000 的规定，本部分与 ISO/IEC 8825-1:2002 相比做了下列编辑性修改：

——"本标准"一词改为"本部分"；

——在引用的标准中，凡已转化为我国标准的各项标准，均用我国的相应标准编号代替。对"规范性引用文件"一章中的标准按 GB/T 1.1—2000 的规定进行了重新排列。

本部分的附录 A、附录 B 和附录 C 是资料性附录。

本部分由中华人民共和国信息产业部提出。

本部分由中国电子标准化研究所归口。

本部分由北京信息工程学院、中国电子技术标准化研究所负责起草。

本部分主要起草人：王凌、郑洪仁、张红。

引　言

GB/T 16262.1、GB/T 16262.2、GB/T 16262.3 和 GB/T 16262.4(抽象语法记法一或 ASN.1)共同规定了定义抽象语法的记法,使应用标准能定义需要传送的信息的类型。它还规定了已定义的类型值规范的记法。

本部分定义了可应用于用 ASN.1 记法定义的类型值的编码规则。应用这些编码规则可产生对这些值的传送语法。这些编码规则规范也隐含着适用于解码。

有多种集合的编码规则可以应用于用 ASN.1 记法定义的类型值。本部分定义了 3 种编码规则集合,分别称为基本编码规则、正则编码规则和非典型编码规则。其中,基本编码规则给出编码发送器如何对数据值进行编码的各种选择,而正则编码规则和非典型编码规则只从为基本编码规则所允许的那些编码中选择一种编码,排除发送器的所有选项。正则编码规则和非典型编码规则加在基本编码规则上的限制集是互不相同的。

如果被编码的值足够小以适于可用的内存,并且需要快速掠过某些嵌套值时,非典型编码规则比正则编码规则更适用。如果需要被编码的值很大,不易适用于可用的内存,或者有必要在整个值成为可用之前对部分值进行编码和发送时,正则编码规则比非典型编码规则更适用。如果编码包含集合值和单一集合值,并且不需要对正则编码规则和非典型编码规则施加限制时,基本编码规则比正则编码规则和非典型编码规则更适用。这是因为后两种编码规则强制要求内存和 CPU 的开销,以便能保证集合值和单一集合值只有一种可能的编码。

附录 A 给出了应用基本编码规则的示例。它不构成本部分的组成部分。

附录 B 总结了在本部分中所产生的客体标识符值的赋值。它不构成本部分的组成部分。

附录 C 给出了对编码实数应用基本编码规则的示例。它不构成本部分的组成部分。

信息技术 ASN.1编码规则 第1部分:基本编码规则(BER)、正则编码规则(CER)和非典型编码规则(DER)规范

1 范围

本部分规定了基本编码规则集合,它们可以用来派生使用GB/T 16262.1、GB/T 16262.2、GB/T 16262.3和GB/T 16262.4规定的记法定义的类型值的传送语法规范,上述这些标准统称为抽象语法记法一或ASN.1。这些基本编码规则也适用于解码这种传送语法,以标识被传送的数据值。该集合还规定了正则编码规则和非典型编码规则集合,它把值的编码局限于只是基本编码规则所提供的替换编码之一。

2 规范性引用文件

下列文件中的条款通过GB/T 16263的本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分,然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

GB/T 1988—1998 信息技术 信息交换用七位编码字符集(eqv ISO/IEC 646:1991)

GB/T 2311—2000 信息技术 字符代码结构和扩充技术(idt ISO/IEC 2022:1994)

GB/T 5261—1994 信息技术 七位和八位编码字符集的控制功能(eqv ISO/IEC 6429:1992)

GB/T 9387.1—1998 信息技术 开放系统互连 基本参考模型 第1部分:基本模型(idt ISO/IEC 7498-1:1994)

GB/T 12054—1989 数据处理 转义序列登记规程(neq ISO 2375:1985)

GB 13000.1—1993 信息技术 通用多八位编码字符集(UCS) 第1部分:体系结构与基本多文种平面(idt ISO/IEC 10646.1:2000)

GB/T 16262.1—2006 信息技术 抽象语法记法一(ASN.1) 第1部分:基本记法规范(ISO/IEC 8824-1:2002, IDT)

GB/T 16262.2—2006 信息技术 抽象语法记法一(ASN.1) 第2部分:信息客体规范(ISO/IEC 8824-2:2002, IDT)

GB/T 16262.3—2006 信息技术 抽象语法记法一(ASN.1) 第3部分:限制规范(ISO/IEC 8824-3: 2002, IDT)

GB/T 16262.4—2006 信息技术 抽象语法记法一(ASN.1) 第4部分:参数化ASN.1规范(ISO/IEC 8824-4: 2002, IDT)

SJ/Z 9047—1987 信息处理 信息交换用字符串形式表示数值的方法 (idt ISO 6093:1985)

要与转义序列一起使用的编码字符集的ISO国际登记簿

3 术语和定义

GB/T 9387.1和GB/T 16262.1中的术语和定义以及下列术语和定义适用于本部分。

3.1

正则编码 canonical encoding

通过应用无实现相关选项的编码规则所得到的抽象值的完整编码。这种规则导致在抽象语法中无歧义和唯一的编码与值之间一对一映射的定义。

3.2

结构化编码 constructed encoding

数据值编码，其中，内容八位位组是一个或多个数据值的完整编码。

3.3

内容八位位组 contents octets

表示特定值的数据值编码的那部分，以便把该特定值与同类型中的其他值区分开。

3.4

数据值 data value

按某个类型值所规定的信息；类型和值用 ASN.1 定义。

3.5

动态一致性 dynamic conformance

在通信场合中，某一实现遵守预定行为的要求的声明。

3.6

(数据值的)编码 encoding (of a data value)

用来表示数据值的八位位组的完整序列。

3.7

内容结束八位位组 end-of-contents octets

在其末端出现的数据值编码的一部分，它用来确定编码的终止。

注：不是所有编码都需要内容结束八位位组。

3.8

标识符八位位组 identifier octets

数据值编码的一部分，它用来标识值的类型。

注：某些 ITU-T 建议把术语"数据元素"用于本八位位组序列，但在本部分中不使用该术语，而其他标准中使用该术语意指"数据值"。

3.9

长度八位位组 length octets

数据值编码的一部分，它紧跟在标识符八位位组的后面，用来确定编码的终止。

3.10

原始编码 primitive encoding

数据值的编码，其中，内容八位位组直接表示该值。

3.11

接收器 receiver

对发送器所产生的八位位组进行解码的一种实现，以便标识出曾编码的数据值。

3.12

发送器 sender

对传送数据值进行编码的一种实现。

3.13

静态一致性 static conformance

对已定义的特性中一组有效特性的某一实现所支持的要求的声明。

3.14

尾0位 trailing 0 bit

位串值中最后位置内的0。

注：由单个0位组成的位串值中的0就是尾0位。移去它将产生一个空的位串。

4 缩略语

下列缩略语适用于本部分。

ASN.1 抽象语法记法一

BER ASN.1的基本编码规则

CER ASN.1的正则编码规则

DER ASN.1的非典型编码规则

ULA 高层体系结构

5 记法

本部分引用GB/T 16262.1定义的记法。

6 约定

6.1 本部分使用术语“最高有效位”和“最低有效位”来规定编码中每个八位位组的值。

注：低层规范使用相同记法来定义串行线路中位传输的次序，或者把这些位赋给并行信道。

6.2 仅为本部分的目的，八位位组中的位编号从8至1，位8为“最高有效位”，位1为“最低有效位”。

6.3 为本部分的目的，两个八位位组串可以进行比较。如果这两个八位位组串的长度相同，并且在每个八位位组位置上的长度相同，则一个八位位组串等于另一个。当且仅当：

a) S_1 和 S_2 在每个位置内具有相同的八位位组，直到并且包括 S_2 内的最后1个八位位组，但 S_1 较长；或者

b) S_1 和 S_2 在一个或多个位置上以及第1个这样的位置具有不同的八位位组，S_i 内的八位位组大于 S_2 内的八位位组，于是认为这些八位位组是无符号二进制数，其位n具有权重 2^{n-1}，则一个八位位组串 S_1 大于另一个 S_2。

7 一致性

7.1 动态一致性在第8章至第12章中规定。

7.2 静态一致性由那些规定了应用一个或多个编码规则的标准来规定。

7.3 基本编码规则允许替换的编码作为发送器的一个选项，声称符合基本编码规则的接收器应支持所有替换的编码。

注：这种替换编码的示例出现在8.1.3.2 b)和表3中。

7.4 正则编码规则或非典型编码规则不允许替换的编码。

8 基本编码结构

8.1 编码的一般规则

8.1.1 编码结构

8.1.1.1 数据值的编码应由下列次序的4种成分组成：

a) 标识符八位位组(见8.1.2)；

b) 长度八位位组(见8.1.3)；

c) 内容八位位组(见8.1.4)；

d) 内容结束八位位组(见 8.1.5)。

8.1.1.2 除非长度八位位组的值需要出现内容结束八位位组,否则该内容结束八位位组不应出现(见 8.1.3)。

8.1.1.3 图 1 示出了编码的结构(原始编码或结构化编码),图 2 示出了替换的结构化编码。

图 1 编码结构

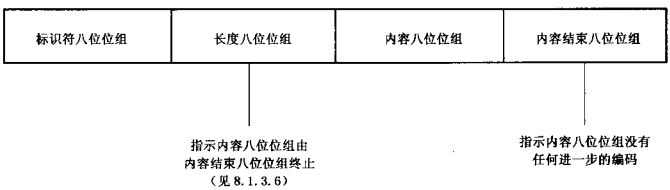


图 2 替换的结构化编码

8.1.1.4 本部分中规定的编码既不受 ASN.1 子类型记法的影响,也不受 ASN.1 类型的可扩充性记法的影响。

注:这意味着当确定编码时,所有约束记法可不予理睬。对于把扩充处理为好像它们曾处于类型的扩充根内的情况,也意味着 CHOICE、SEQUENCE 和 SET 中的所有可扩充性标记可不予理睬。

8.1.2 标识符八位位组

8.1.2.1 标识符八位位组应对数据值类型的 ASN.1 标签(类和编号)进行编码。

8.1.2.2 对于编号范围为 0～30(包括 0 和 30)的标签,标识符八位位组应由如下单个八位位组编码构成:

a) 位 8 和位 7 应编码为用来表示表 1 规定的标签类;

b) 按 8.1.2.5 的规则,位 6 应为 0 或 1;

c) 位 5 至位 1 应把标签编号编码为二进制整数,位 5 是最高有效位。

表 1 标签类的编码

类	位 8	位 7
通用	0	0
应用	0	1
上下文特定	1	0
专用	1	1

8.1.2.3 图 3 示出了带有一个编号范围在 0～30(包括 0 和 30)的标签的类型的标识符八位位组形式。

8.1.2.4 对于编号大于或等于 31 的标签,标识符八位位组应包含一个引导八位位组及后随的一个或多个后继八位位组。

8.1.2.4.1 引导八位位组应编码如下:

a) 位 8 和位 7 应编码为用来表示表 1 列出的标签类;

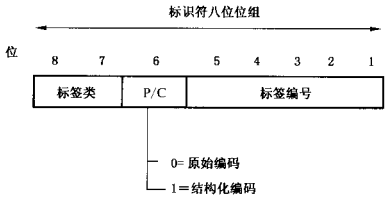


图 3 标识符八位位组(低标签编号)

b) 按 8.1.2.5 的规则,位 6 应为 0 或 1;

c) 位 5 至位 1 应编码为 11111_2。

8.1.2.4.2 后继八位位组应把标签编号编码如下:

a) 除了最后 1 个标识符八位位组外,每个八位位组的位 8 应置 1;

b) 第 1 个后继八位位组的位 7 至位 1,后随第 2 个后继八位位组的位 7 至位 1,依次后随每个更后面的八位位组的位 7 至位 1,直到并包括标识符八位位组中的最后 1 个后继八位位组,应是等于标签编号的无符号二进制整数的编码,以第 1 个后继八位位组的位 7 为最高有效位;

c) 第 1 个后继八位位组的位 7 至位 1 不应都为 0。

8.1.2.4.3 图 4 示出了带有一个编号大于 30 的标签的类型的标识符八位位组形式。

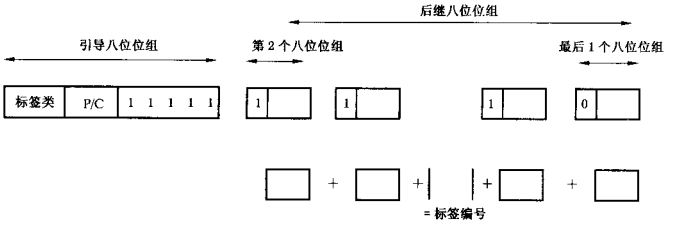


图 4 标识符八位位组(高标签编号)

8.1.2.5 若编码是原始编码,则位 6 置为 0,若编码是结构化编码,则位 6 置为 1。

注:对每种类型,以后各条规定了编码是原始编码还是结构化编码。

8.1.2.6 GB/T 16262.1—2006 规定,使用关键字 CHOICE 定义的类型的标签采用类型的标签值,而类型的标签值采用已选定的数据值。

8.1.2.7 GB/T 16262.2—2006 的 14.2 和 14.4 中规定,如果"ObjectClassFieldType"是类型字段、可变类型值字段或可变类型值集合字段,则使用"ObjectClassFieldType"定义的类型的标签是不确定的。该类型随后定义为 ASN.1 类型,然后其完整编码等同于所赋类型的值的完整编码(包括标识符八位位组)。

8.1.3 长度八位位组

8.1.3.1 规定两种长度八位位组形式,它们是:

a) 确定形式(见 8.1.3.3);及

b) 不定形式(见 8.1.3.6)。

8.1.3.2 如果编码

a) 是原始编码,则发送器应使用确定形式(见 8.1.3.3);

b) 是结构化编码且都是立即可用的，则发送器应使用确定形式（见 8.1.3.3）或不定形式（见 8.1.3.6），作为发送器的一个选项；

c) 是结构化编码且不都是立即可用的，则发送器应使用不定形式（见 8.1.3.6）。

8.1.3.3 对于确定形式，长度八位位组应由一个或多个八位位组组成，并应表示使用短形式（见 8.1.3.4）或长形式（见 8.1.3.5）作为发送器一个选项的内容八位位组中的八位位组数。

注：若内容八位位组中的八位位组数小于或等于 127 时，仅使用短形式。

8.1.3.4 在短形式中，长度八位位组应由单个八位位组组成，其中位 8 为 0，位 7 至位 1 把内容八位位组（它们可能是 0）中的八位位组数编码为无符号二进制整数，以位 7 为最高有效位。

例：$L=38$ 的编码为 00100110_2。

8.1.3.5 在长形式中，长度八位位组应由一个初始八位位组和一个或多个后继八位位组组成。初始八位位组应编码如下：

a) 位 8 应为 1；

b) 位 7 至位 1 应把长度八位位组中的后继八位位组数编码为无符号二进制整数，以位 7 为最高有效位；

c) 应不使用值 11111111_2。

注：引入这个限制是为了将来可能的扩展。

第 1 个后继八位位组的位 8 至位 1，后随第 2 个后继八位位组的位 8 至位 1，依次后随更后面八位位组的位 8 至位 1，直至并包含最后 1 个后继八位位组，应是等于内容八位位组中八位位组数的无符号二进制整数的编码，以第 1 个后继八位位组的位 8 为最高有效位。

例：$L=201$ 可编码为

$$10000001_2$$

$$11001001_2$$

注：在长形式中，是否使用比最少的必需数更多的长度八位位组是发送器的一个选项。

8.1.3.6 对于不定形式，长度八位位组指示内容八位位组由内容结束八位位组来终止（见8.1.5），并应由单个八位位组组成。

8.1.3.6.1 单个八位位组的位 8 应置为 1，位 7 至位 1 置为 0。

8.1.3.6.2 若使用该长度形式，则应在内容八位位组之后的编码中出现内容结束八位位组（见8.1.5）。

8.1.4 内容八位位组

内容八位位组应由 0 个、1 个或多个八位位组组成，并且应编码后续各条规定的数据值。

注：内容八位位组依赖于数据值的类型；后续各条遵循与 ASN.1 中相同的类型定义序列。

8.1.5 内容结束八位位组

若长度按 8.1.3.6 的规定编码，则应出现内容结束八位位组，否则应不出现。

内容结束八位位组应由两个值为 0 的八位位组组成。

注：内容结束八位位组可被认为是值的编码，其标签为通用类的，形式为原始编码，标签号为 0，且内容不存在，因此：

内容结束八位位组	长度	内容
00_{16}	00_{16}	无

8.2 布尔值的编码

8.2.1 布尔值的编码应是原始编码。内容八位位组由单个八位位组组成。

8.2.2 若布尔值是 FALSE，则八位位组应为 0。

若布尔值是 TRUE，则八位位组应为任意非 0 值，作为发送器的一个选项。

例：若是 BOOLEAN 类型，值 TRUE 被编码为：

布尔	长度	内容
01_{16}	01_{16}	FF_{16}

8.3 整数值的编码

8.3.1 整数值的编码应是原始编码，内容八位位组由一个或多个八位位组组成。

8.3.2 若整数值编码的内容八位位组由多个八位位组组成，则第1个八位位组的各个位和第2个八位位组的位8：

a) 应不全为1；并且

b) 应不全为0。

注：这些规则确保整数值总是用最小可能的八位位组数进行编码。

8.3.3 内容八位位组应是等于整数值的对2的补码的二进制数，其组成是由第1个八位位组的位8至位1，后随第2个八位位组的位8至位1，依次后随每个八位位组的位8至位1，直到并包含内容八位位组的最后1个八位位组。

注：2的补码的二进制数的值通过计数内容八位位组中的位得出：计数从最后1个八位位组的位1开始作为位0，到第1个八位位组的位8结束。每位赋予一个2^N的数值，这里N是该位在上面计数序列中的位置。2的补码的二进制数的值是：累加计算那些置1的位的数值，但不包括第1个八位位组的位8，然后，若第1个八位位组的位8置为1，则这个累加值减去第1个八位位组的位8的数值所得的结果。

8.4 枚举值的编码

枚举值的编码应是与之相关的整数值的编码。

注：它是原始编码。

8.5 实数值的编码

8.5.1 实数值的编码应是原始编码。

8.5.2 如果实数值为0值，则编码中应没有内容八位位组。

8.5.3 对非0实数值，如果抽象值的基数是10，则编码值的基数也应为10，如果抽象值的基数是2，则编码值的基数应为2、8或16，作为发送器的一个选项。

8.5.4 如果实数值为非0值，那么用于编码的基数应为8.5.3规定的B′。如果B′是2、8或16，应使用8.5.6规定的二进制编码。如果B′是10，则应使用8.5.7规定的字符编码。

8.5.5 第1个内容八位位组的位8应设置如下：

a) 如果位8=1，则使用8.5.6规定的二进制编码；

b) 如果位8=0，且位7=0，则使用8.5.7规定的十进制编码；

c) 如果位8=0，且位7=1，则按8.5.8的规定编码一个“SpecialRealValue”(见GB/T 16262.1)。

8.5.6 当使用二进制编码时(位8=1)，如果尾数M是非0，则它应由一个符号S、一个非负整数值N以及一个二进制比例因子F来表示，诸如：

$$M = S \times N \times 2^F$$

$$0 \leqslant F < 4$$

$$S = +1 \text{ 或 } -1$$

注：在某些环境下需要二进制比例因子F，以便将尾数隐含的小数点与本条编码规则所要求的位置对齐。这种对齐不能总是通过修改指数E来获得。如果用于编码的基数B'是8或16，隐含的小数点只能通过改变指数E分别以3个位或4个位为一步进行移动。因此，可能要求不是0的二进制比例因子的值，以便将隐含的小数点移动到所要求的位置。

8.5.6.1 如果S为−1，第1个内容八位位组的位7应为1，否则为0。

8.5.6.2 第1个内容八位位组的位6至位5应编码基数B'的值如下：

位 6 至位 5	基数
0 0	基数为 2
0 1	基数为 8
1 0	基数为 16
1 1	为本部分将来版本保留

8.5.6.3 第 1 个内容八位位组的位 4 至位 3 应把二进制比例因子 F 的值编码为无符号二进制整数。

8.5.6.4 第 1 个内容八位位组的位 2 至位 1 应编码指数格式如下：

a) 如果位 2 至位 1 为 00，那么第 2 个内容八位位组把指数的值编码为 2 的补码的二进制数；

b) 如果位 2 至位 1 为 01，那么第 2 个和第 3 个内容八位位组把指数的值编码为 2 的补码的二进制数；

c) 如果位 2 至位 1 为 10，那么第 2、第 3 和第 4 个内容八位位组把指数的值编码为 2 的补码的二进制数；

d) 如果位 2 至位 1 为 11，那么第 2 个内容八位位组编码用于编码指数的值的八位位组的数，假定为 X，(为无符号二进制数)，并且第 3 个直到第(X 加 3)个(包括二者)内容八位位组将指数的值编码为 2 的补码的二进制数；X 的值应至少为 1，发送指数的最前 9 位应不全为 0 或不全为 1。

8.5.6.5 剩余的内容八位位组将整数 N(见 8.5.6)的值编码为无符号二进制数。

注 1：对于非正则 BER，没有尾数的浮点常规化的需求。这允许实现者发送包含尾数的八位位组，而不用在内存中对尾数执行移位功能。在正则编码规则和非典型编码规则中，规定了常规化，并且尾数(除非它是 0)需要重复地移位直至最低有效位为 1。

注 2：实数数字的这种表示与通常用在浮点硬件中的格式有很大不同，但实数数字的表示已设计成能容易地与这种格式来回地转换(见附录 C)。

8.5.7 当使用十进制编码时(位 8 至位 7=00)，按 SJ/Z 9047—1987 中使用的术语，跟在第 1 个内容八位位组后的所有内容八位位组形成作为发送器一个选项的字段长度，并且按照 SJ/Z 9047—1987 进行编码。SJ/Z 9047—1987 数字表示的选择由第 1 个内容八位位组的位 6 至位 1 规定如下：

位 6 至位 1	数字表示
00 0001	SJ/Z 9047 NR1 形式
00 0010	SJ/Z 9047 NR2 形式
00 0011	SJ/Z 9047 NR3 形式

位 6 至位 1 中剩余的值为本部分而保留。

应不使用伴随文件(见 SJ/Z 9047—1987)规定的比例因子。

注 1：在 SJ/Z 9047—1987 中关于至少使用一个数字用到十进制标记的左边的建议，在本部分中也建议这么做，但并不是强制的。

注 2：使用常规化形式(见 SJ/Z 9047—1987)是发送器的一个选项，这并不重要。

8.5.8 当“SpecialRealValues”被编码(位 8 至位 7=01)时，应只有一个内容八位位组，有如下值：

01000000 值为 **PLUS-INFINITY**

01000001 值为 **MINUS-INFINITY**

位 8 至位 7 等于 0 和 1 的所有其他值分别为本部分的补篇而保留。

8.6 位串值的编码

8.6.1 位串值的编码应是原始编码，或是结构化编码，作为发送器的选项。

注：在整个位串可用之前有必要传送部分位串时，使用结构化编码。

8.6.2 原始编码的内容八位位组应包含一个初始八位位组，后随 0 个、1 个或多个后继八位位组。

8.6.2.1 从引导位开始直到结尾位的位串值中的所有位，应置于第 1 个后继八位位组的位 8 至位 1，后随第 2 个后继八位位组的位 8 至位 1，依次后随每个八位位组的位 8 至位 1，再后随从位 8 开始的最

后1个后继八位位组需要的一些位。

注：术语"引导位"和"结尾位"在GB/T 16262.1—2006的21.2中定义。

8.6.2.2 作为以位1为最低有效位的无符号二进制整数，初始八位位组应编码最后1个后继八位位组中未使用位的数。该数的范围应为0到7。

8.6.2.3 若位串为空，应没有后继的八位位组，且初始八位位组应为0。

8.6.2.4 在应用GB/T 16262.1—2006中的21.7时，BER编码器/解码器可以增加值的尾0位或从值中删去尾0位。

注：如果位串值没有置为1的若干位，那么编码器(作为发送器的选项)可以用一个长度为1和一个初始八位位组置为0来编码该值，或者可以将该值编码成带有一个或多个置为0的位后随初始八位位组。

8.6.3 结构化编码的内容八位位组应由0个、1个或多个嵌套的编码组成。

注：每个这样的编码包括标识符、长度和内容八位位组，若它是结构化编码，则还可能包括内容结束八位位组。

8.6.4 为用此方法编码位串值，应将其分段。每个段应由该值的一系列连续位组成，除最后一段外，应包含8的整数倍的位数。整个值中的每一位应精确地处于某一段内，但不应把有效位放在段边界上。

注：段可能是0长度的，即不包含任何位。

8.6.4.1 内容八位位组中的每个编码应表示整个位串的一个段，该编码出自本条的一种递归应用。在该递归应用中，把每个段处理为一个位串值。段的编码应按照这些位在整个值中的次序出现在内容八位位组中。

注1：作为该递归的结果，内容八位位组中的每个编码本身可能是原始编码或结构化编码。然而，通常这样的编码将是原始编码。

注2：实际上，内容八位位组的标签总是通用类，编号为3。

8.6.4.2 示例

若是类型 **BIT STRING**，值**'0A3B5F291CD'H** 可以如下编码。在该示例中，位串表示是原始编码：

位串	长度	内容
03_{16}	07_{16}	$040A3B5F291CD0_{16}$

上面示出的值也可以如下编码，在该示例中，位串表示是结构化编码：

位串	长度	内容		
23_{16}	80_{16}			
		位串	长度	内容
		03_{16}	03_{16}	$000A3B_{16}$
		03_{16}	05_{16}	$045F291CD0_{16}$
EOC	长度			
00_{16}	00_{16}			

8.7 八位位组串值的编码

8.7.1 八位位组串值的编码应是原始编码或是结构化编码，作为发送器的选项。

注：在整个八位位组串可用之前有必要传送部分八位位组串时，使用结构化编码。

8.7.2 原始编码包含0个、1个或多个值等于数据值中八位位组的内容八位位组，按照数据值中八位位组出现的次序，并使该数据值的八位位组的最高有效位与内容八位位组的一个八位位组的最高有效位对齐。

8.7.3 结构化编码的内容八位位组应由0个、1个或多个编码组成。

注：每个这样的编码包括标识符、长度和内容八位位组。若它是结构化编码，则还可能包括内容结束八位位组。

8.7.3.1 为用此方法编码一个八位位组串值，将其分段。每个段应由该值的一系列连续八位位组组成。不应把有效位放在段边界上。

注：段可能是0长度的，即不包含任何八位位组。

8.7.3.2 内容八位位组中的每个编码应表示整个八位位组串的一个段，该编码出自本条的一种递归应用。在该递归应用中，把每个段处理为一个八位位组串值。段的编码应按照这些位在整个值中的次序出现在内容八位位组中。

注1：作为该递归的结果，内容八位位组中的每个编码本身可能是原始编码或结构化编码。然而，通常这样的编码将是原始编码。

注2：实际上，内容八位位组的标签总是通用类，编号为4。

8.8 空值的编码

8.8.1 空值的编码应是原始编码。

8.8.2 内容八位位组应不包含任何八位位组。

注：长度八位位组为0。

例：若是 **NULL** 类型，**NULL** 值可以编码为：

NULL	长度
05_{16}	00_{16}

8.9 序列值的编码

8.9.1 序列值的编码应是结构化编码。

8.9.2 内容八位位组应由 ASN.1 序列类型定义中列出的每个类型的一个数据值的完整编码组成，除非引用的类型带有关键字 **OPTIONAL** 或 **DEFAULT**，否则这些编码按定义中的次序出现。

8.9.3 引用的类型带有关键字 **OPTIONAL** 或 **DEFAULT**，其数据值的编码可以出现，但不是必要的。若出现，则它应在按 ASN.1 定义的类型的编码的相应点上出现。

例：若类型为：

SEQUENCE{name IA5 string, ok BOOLEAN}

值为：

{name "Smith", ok TRUE}

可以编码为：

Sequence	Length	Contents		
30_{16}	$0A_{16}$			
		IA5String	Length	Contents
		16_{16}	05_{16}	"Smith"
		Boolean	Length	Contents
		01_{16}	01_{16}	FF_{16}

8.10 单一序列值的编码

8.10.1 单一序列值的编码应是结构化编码。

8.10.2 内容八位位组应由0个、1个或多个在 ASN.1 定义中列出的类型的数据值的完整编码组成。

8.10.3 数据值编码的次序应与被编码的单一序列值中数据值的次序相同。

8.11 集合值的编码

8.11.1 集合值的编码应是结构化编码。

8.11.2 内容八位位组应由 ASN.1 集合类型定义中列出的每个类型的一个数据值的完整编码组成。除非引用的类型带有关键字 **OPTIONAL** 或 **DEFAULT**，否则这些编码按发送器选定的次序出现。

8.11.3 引用的类型带有关键字 **OPTIONAL** 或 **DEFAULT**，其数据值编码可以出现，但不是必要的。

注：集合值中的数据值的次序不重要，对传送期间的次序没有限制。

8.12 单一集合值的编码

8.12.1 单一集合值的编码应是结构化编码。

8.12.2 同 8.10.2。

8.12.3 编码及后续解码时，不必保持数据值的次序。

8.13 选择值的编码

选择值的编码应与被选择的类型值的编码相同。

注 1：依照被选择的类型而定，编码可以是原始编码或结构化编码。

注 2：按照 ASN.1 选择类型定义的规定，用于标识符八位位组的标签是被选择的类型的标签。

8.14 有标签值的编码

8.14.1 有标签值的编码应由 8.14.2 和 8.14.3 中规定的“TaggedType”记法中出现的类型所对应数据值的完整编码(称为基编码)导出。

8.14.2 若类型定义中未使用隐式的标签(见 GB/T 16262.1—2006 的 30.6)，则编码应是结构化编码，内容八位位组应是完整的基编码。

8.14.3 若类型定义中使用了隐式标签，则：

a) 若基编码是结构化编码，则编码也应是结构化编码，否则应是原始编码；

b) 内容八位位组应与基编码的内容八位位组相同。

示例：

由 ASN.1 类型定义(在一个显式标签的环境中)：

Type 1::= VisibleString

Type 2::= [APPLICATION 3] IMPLICIT Type 1

Type 3::= [2] Type 2

Type 4::= [APPLICATION 7] IMPLICIT Type 3

Type 5::= [2] IMPLICIT Type 2

值**“Jones”**编码如下：

对 Type 1：

VisibleString	Length	Contents
$1A_{16}$	05_{16}	$4A6F6E6573_{16}$

对 Type 2：

[APPLICATION 3]	Length	Contents
43_{16}	05_{16}	$4A6F6E6573_{16}$

对 Type 3：

[2]	Length	Contents		
$A2_{16}$	07_{16}			
		[APPLICATION 3]	Length	Contents
		43_{16}	05_{16}	$4A6F6E6573_{16}$

对 Type 4：

[APPLICATION 7]	Length	Contents		
67_{16}	07_{16}			
		[APPLICATION 3]	Length	Contents
		43_{16}	05_{16}	$4A6F6E6573_{16}$

对 Type 5：

[2]	Length	Contents
82_{16}	05_{16}	$4A6F6E6573_{16}$

8.15 开放类型的编码

开放类型的值也是某一(其他)ASN.1 类型的值。这种值的编码应是在此为认为是其他类型的值

而规定的完整编码。

8.16 单一实例值的编码

8.16.1 单一实例值的编码应是下列带有 8.16.2 规定的值的序列类型的 BER 编码。

```
[UNIVERSAL 8] IMPLICIT SEQUENCE {
        type-id     <DefinedObjectClass>.&id,
        value [0]   EXPLICIT   <DefinedObjectClass>.&Type
    }
```

其中,"<DefinedObjectClass>"被用于"InstanceOfType"记法的特定"DefinedObjectClass"所替换。

注:当值是单个 ASN.1 类型的值,并且使用 BER 编码时,该类型的编码等同于外部类型的对应值的编码,其中替换的语法是指用来表示该抽象值。

8.16.2 8.16.1 中的序列类型的成分值应与 GB/T 16262.2—2006 的 C.7 中相关类型的对应成分的值相同。

8.17 嵌入式 pdv 类型值的编码

8.17.1 嵌入式 pdv 类型值的编码应是在 GB/T 16262.1—2006 的 33.5 中定义的类型的 BER 编码。

8.17.2 **data-value OCTET STRING** 的内容应是使用已标识的传送语法的嵌入式 pdv 类型(见 GB/T 16262.1—2006 中的 33.3a))的抽象数据值的编码,并且所有其他字段的值应与出现在抽象值中的值相同。

8.18 外部类型值的编码

8.18.1 外部类型值的编码应是假设定义在 **EXPLICIT TAGS** 环境中,其值按如下规定的序列类型的 BER 编码。

```
[UNIVERSAL 8]  IMPLICIT SEQUENCE  {
  direct-reference          OBJECT IDENTIFIER OPTIONAL,
  indirect-reference        INTEGER OPTIONAL,
  data-value-descriptor     ObjectDescriptor OPTIONAL,
  encoding                  CHOICE  {
  single-ASN1-type              [0] ABSTRACT-SYNTAX.&Type,
  octet-aligned                 [1] IMPLICIT OCTET STRING,
  arbitrary                     [2] IMPLICIT BIT STRING } }
```

注:由于历史原因,该序列类型与 GB/T 16262.1 中规定的序列类型不同。

8.18.2 字段的值依赖于要发送的抽象值,也即在 GB/T 16262.1—2006 中的 34.5 中规定的类型的值。

8.18.3 当且仅当 **data-value-descriptor** 出现在抽象值中,并且应有相同的值时,上述 **data-value-descriptor** 应出现。

8.18.4 上述 **direct-reference** 和 **indirect-reference** 的值应按照表 2 来出现或不存在。表 2 把 GB/T 16262.1—2006中的 34.5 中定义的外部类型替换的标识映射成 18.8.1 中定义的外部类型成分的 **direct-reference** 和 **indirect-reference**。

表 2 标识用的替换的编码

identification	direct-reference	indirect-reference
syntaxes	* * * 不能出现 * * *	* * * 不能出现 * * *
syntax	syntax	不存在
presentation-context-id	不存在	presentation-context-id
context-negotiation	传送语法	presentation-context-id

表 2(续)

identification	direct-reference	indirect-reference
transfer-syntax	* * * 不能出现 * * *	* * * 不能出现 * * *
fixed	* * * 不能出现 * * *	* * * 不能出现 * * *

8.18.5 数据值应按照编码标识的传送语法进行编码，并应将该数据值放入下面规定的替换的编码选择中。

8.18.6 如果数据值是单个 ASN.1 数据类型的值，并且用于该数据类型的编码规则是本部分中规定的编码规则之一，则发送实现应使用下列任何编码选择：

- 单个 ANS.1 类型
- 八位位组对齐的
- 任意的

作为一实现选项。

8.18.7 如果使用商定的或协商的编码规则的数据值的编码是八位位组的整数倍，则发送实现应使用下列任何编码选择：

- 八位位组对齐的
- 任意的

作为一实现选项。

注：一系列 ASN.1 类型的，并且传送语法规定了通过将 ASN.1 基本编码规则应用于每个 ASN.1 类型所产生的八位位组串的原始拼接的数据值归入该范畴，而不是归入 8.18.6 的范畴。

8.18.8 如果使用商定的或协商的编码规则的数据值的编码不是八位位组的整数倍，则编码选择应是：

- 任意的

8.18.9 如果编码的选择是单个 ANS.1 类型，那么 ASN.1 类型应替换开放类型，其值等于要编码的数据值。

注：可能出现在开放类型中的值的范围通过与 **direct-reference** 相关的客体标识符值，和/或与 **indirect-reference** 相关整数值的注册来确定。

8.18.10 如果编码的选择选定为八位位组对齐的，那么，数据值应按照商定的或协商的编码传送语法进行编码，所得出的八位位组应形成八位位组串的值。

8.18.11 如果编码的选择是任意的，那么，数据值应按照商定的或协商的编码传送语法进行编码，其结果应形成位串的值。

8.19 客体标识符值的编码

8.19.1 客体标识符值的编码应是原始编码。

8.19.2 内容八位位组应是一起拼接的子标识符(见 8.19.3 和 8.19.4)的编码的(有序)列表。

每个子标识符表示一系列(1 个或多个)八位位组。每个八位位组的位 8 指示它是否为该系列的最后 1 个八位位组：最后八位位组的位 8 为 0；前面的每个八位位组的位 8 为 1。序列中这些八位位组的位 7 到位 1 共同编码为子标识符。在概念上，这些位被拼接起来，以形成一个无符号的二进制数，其最高有效位是第 1 个八位位组的位 7，最低有效位是最后 1 个八位位组的位 1，子标识符应尽可能最少地用八位位组来编码，也就是说，子标识符的引导八位位组应没有值 80_{16}。

8.19.3 子标识符的编号(N)应比被编码的客体标识符值中的客体标识符的成分的编号少 1。

8.19.4 第 1 个子标识符的数值从被编码的客体标识符值中的前两个客体标识符成分的值导出。使用公式

$$(X \times 40) + Y$$

其中：X 是第 1 个客体标识符成分的值，Y 是第 2 个客体标识符成分的值。

注：这种前两个客体标识符成分的组合认可的只有三个值由根结点赋予，且由 $X=0$ 和 $X=1$ 达到的结点最多赋于 39 个后继值。

8.19.5 第 i 个子标识符($2 \leqslant i \leqslant N$)的数值是第($i+1$)个客体标识符成分的数值。

示例：**OBJECT IDENTIFIER** 的值

{**joint-iso-itu-t 100 3**}

它与下式相同

{**2 100 3**}

其第 1 个子标识符为 180，第 2 个子标识符为 3。所得到的编码为：

OBJECT IDENTIFIER	**Length**	**Contents**
06_{16}	03_{16}	813403_{16}

8.20 相关客体标识符值的编码

注：相关客体标识符中的客体标识符成分的编码与客体标识符中成分(在第 2 个之后)的编码相同。

8.20.1 相关客体标识符值的编码应是原始编码。

8.20.2 内容八位位组应是一起拼接的子标识符(见 8.20.3 和 8.20.4)的编码的(有序的)列表。每个子标识符表示一系列(1 个或多个)八位位组。每个八位位组的位 8 指示其是否是系列中的最后 1 个八位位组：最后 1 个八位位组的位 8 是 0，前面的每个八位位组的位 8 为 1。序列中这些八位位组的位 7 至位 1 共同编码为子标识符。在概念上，这些位的组被拼接起来，以形成一个无符号的二进制数，其最高有效位是第 1 个八位位组的位 7，最低有效位是最后 1 个八位位组的位 1。子标识符应尽可能最少地用八位位组来编码，也就是说，子标识符的引导八位位组应没有值 80_{16}。

8.20.3 子标识符的编号(N)应等于要被编码的相关客体标识符值中的客体标识符的编号。

8.20.4 第 i 个子标识符($1 \leqslant i \leqslant N$)的数据值是要被编码的相关客体标识符值中的第 i 个客体标识符的数据值。

8.20.5 示例，一个相关客体标识符值为：

{ **8571 3 2**}

其子标识符为 **8571**、**3** 和 **2**。所得到得编码为：

RELATIVE OID	**Length**	**Contents**
$0D_{16}$	04_{16}	$C27B0302_{16}$

8.21 受限字符串类型值的编码

8.21.1 数据值由 ASN.1 类型定义中规定的字符集中的字符串组成。

8.21.2 每个数据值应编码为独立于同一类型的其他数据值。

8.21.3 每个字符串类型应按如下说明的方式进行编码：

[**UNIVERSAL x**] **IMPLICIT OCTET STRING**

其中，x 是指派给 GB/T 16262.1—2006 中的字符串类型的通用类标签编号。八位位组串的值在 8.21.4 和 8.21.5 中规定。

8.21.4 在 GB/T 16262.1—2006 中，若直接引用一个枚举表(**NumericString** 和 **PrintableString**)来规定字符串类型，则八位位组串的值应是在 8.21.5 中为带有相同字符串值的 **VisibleString** 类型规定的值。

8.21.5 对于除 **UniversalString** 和 **BMPString** 串之外的受限字符串，八位位组串应包含 GB/T 2311 中为 8 位环境的编码所规定的八位位组，使用按照 GB/T 12054 登记的转义序列和字符编码。

8.21.5.1 除非在 GB/T 16262.1—2006 中用来定义字符串类型的登记号之一中有规定的转义序列，否则不使用转义序列。

8.21.5.2 在每串的开始处，某些登记号应被假设为指明的 G0 和/或 C0 和/或 C1，且被调用(使用

GB/T 2311 的术语)。表 3 将对每个类型以及它们隐式的假定的转义序列加以规定。

8.21.5.3 某些字符集串类型的编码中应不包含显式转义序列;在所有其他情况下,8.21.5.1 允许的任何转义序列可以在任何时候出现,包括在编码的开始处。表 3 列出允许有其显式转义序列的类型。

表 3 转义序列的使用

类 型	假定的 G0 (登记号)	假定的 C0 和 C1 (登记号)	假定的转义序列和锁定 移位(在可用处)	是否允许 显式转义序列
NumericString	6	无	ESC 2/8 4/2 LS0	否
PrintableString	6	无	ESC 2/8 4/2 LS0	否
TeletexString (T61String)	102	106(C0) 107(C1)	ESC 2/8 7/5 LS0 ESC 2/1 4/5 ESC 2/2 4/8	是
VideotexString	102	1(C0) 73(C1)	ESC 2/8 7/5 LS0 ESC 2/1 4/0 ESC 2/2 4/1	是
VisibleString (GB/T 1988)	6	无	ESC 2/8 4/2 LS0	否
IA5String	6	1(C0)	ESC 2/8 4/2 LS0 ESC 2/1 4/0	否
GraphicString	6	无	ESC 2/8 4/2 LS0	是
GeneralString	6	1(C0)	ESC 2/8 4/2 LS0 ESC 2/1 4/0	是

注:有许多通常使用的字符(例如,A 到 Z)出现在具有各个登记号和转义序列的许多字符表中。当 ASN.1 类型允许转义序列时,对一个特定的字符串有多种编码是可能的(见 7.3)。

8.21.5.4 应不使用宣布符,除非 ASN.1 用户有明确允许。

注:ASN.1 类型的选择还提供了一个宣布符功能度的有限形式。特定应用协议可以选择,以便在其他协议要素中携带宣布符或者详细地规定使用宣布符的方式。

示例:这个示例的类型定义为:

Name ::= VisibleString

其值为

"Jones"

可被编码(原始编码形式)为:

VisibleString	Length	Contents
$1A_{16}$	05_{16}	$4A6F6E6573_{16}$

或(结构化编码形式,确定长度)为:

VisibleString	Length	Contents		
$3A_{16}$	09_{16}			
		OctetString	Length	Contents
		04_{16}	03_{16}	$4A6F6E_{16}$
		OctetString	Length	Contents
		04_{16}	02_{16}	6573_{16}

或(结构化编码形式,不定长度)为:

VisibleString	Length	Contents		
$3A_{16}$	09_{16}			
		OctetString	Length	Contents
		04_{16}	03_{16}	$4A6F6E_{16}$
		OctetString	Length	Contents
		04_{16}	02_{16}	6573_{16}
		EOC	Length	
		00_{16}	00_{16}	

8.21.6 上述示例示出了三种(更多)可能的有效形式,作为发送器的一个选项。要求接收器处理所有允许的形式(见 7.3)。

8.21.7 对 **UniversalString** 类型,八位位组串应包含在 GB 13000.1—1993 中规定的使用 4 个八位位组正则形式(见 GB 13000.1—1993 中的 13.2)的八位位组。不应使用特定符号。如果控制功能满足被 8.21.9施加的限制,则可以使用该控制功能。

8.21.8 对 **BMPString** 类型,八位位组串应包含在 GB 13000.1—1993 中规定的使用 2 个八位位组 BMP 形式(见 GB 13000.1—1993 中的 13.1)的八位位组。不应使用特定符号。如果控制功能满足被 8.21.9 施加的限制,则可以使用该控制功能。

8.21.9 在下列例外的情况下,可以使用 GB/T 5261—1994 中的 C0 和 C1 控制功能。

注 1:本条的效果是当禁止对其他字符集使用转义时,允许有用的控制功能,例如:LF、CR、TAB 等。

注 2:对 BMPString,C0 和 C1 控制功能被编码为两个八位位组,对 UniversalString,C0 和 C1 控制功能被编码为四个八位位组。

a) 应不使用 GB/T 2311—2000 中定义的宣布符转义序列。

注 3:假设的字符编码环境是 GB 13000.1。

b) 应不使用 GB/T 2311—2000 中定义的指明或标识转义序列,包括 GB 13000.1—1993 的 17.2 和 17.4 所允许的标识转义序列。

注 4:ASN.1 允许使用 PermittedAlphabet 子类型记法来选择允许的字符集。PermittedAlphabet 也用来选择 GB 13000.1的实现级别。**BMPString** 总是用于两个八位位组的形式、**UniversalString** 总是用于四个八位位组的形式。

c) 应不使用调用 GB/T 2311—2000 的转义序列或控制序列,例如 SHIFT IN(SI)、SHIFT OUT (SO)或 LOCKING SHIFT FOR G3(SS3)。

d) 编码应与 GB 13000.1 一致,并保留在该代码集中。

e) 应不使用按照 GB 13000.1—1993 的 16.3 标识图形字符子集的控制序列。

注 5:ASN.1 的应用使用划分子类型来指示 GB 13000.1 图形字符的子集,和选择与 GB/T 2311 控制字符相对应的 GB 13000.1 字位。

f) GB 13000.1—1993 的 16.5 转义序列不应被用于切换到 GB/T 2311 代码。

8.21.10 对于 **UTF8String** 类型,八位位组串应包含 GB 13000.1—1993 中的附录 D 中规定的八位位组。不应使用宣布符和转义序列,并且每个字符应按对该字符有效的最小数的八位位组进行编码。

8.22 无限制字符串类型值的编码

8.22.1 无限制字符串类型值的编码应是 GB/T 16262.1—2006 中的 40.5 定义的类型的 BER 编码。

8.22.2 string-value OCTET STRING 的内容应是使用已标识的字符传送语法的无限制字符串类型(见 GB/T 16262.1—2006 中的 40.3a))的抽象字符串值的编码,并且所有其他字段的值应与该抽象值中出现值相同。

8.23 下列"有用的类型"应编码为已经用 GB/T 16262.1—2006 中的 42 至 44 中给出的定义所替代:

- 通用时
- 世界协调时

- 客体描述符

9 正则编码规则

正则编码规则使用的数据值的编码是第8章描述的基本编码及下列的限制，这些限制也在第11章中列出。

9.1 长度形式

如果编码是结构化编码，则应使用不定长度形式。如果编码是原始编码，应包括必要的最短长度的八位位组[与8.1.3.2 b)对比]。

9.2 串编码形式

如果位串、八位位组串和受限字符串的值要求不大于1000个内容八位位组，则应使用原始编码对它们进行编码，否则，应使用结构化编码。结构化编码中包含的串分片应使用原始编码进行编码。每个分片的编码，除了可能的最后一个分片外，应具有1000个内容八位位组(与8.21.6对比)。

9.3 集合成分

集合值的成分值的编码应按照GB/T 16262.1—2006中的8.6中规定的标签所确定的次序出现。此外，当一个或多个成分是无标签的选择类型时，为确定成分的编码次序，每个无标签的选择类型也被排序，好像该类型有一个与该选择类型或其中嵌套的任何无标签选择类型中的最小标签相等的标签。

示例：

假设有一个 **IMPLICIT TAGS** 的置标签环境：

```
A ::= SET
        {
        a     [3]  INTEGER,
        b     [1]  CHOICE
                        {
                        c     [2]  INTEGER,
                        d     [4]  INTEGER
                        },
        e     CHOICE
                        {
                        f     CHOICE
                              {
                              g     [5]     INTEGER,
                              h     [6]     INTEGER
                              },
                        i     CHOICE
                              {
                              j     [0]     INTEGER
                             }
                        }
        }
```

编码集合成分的次序将总是e、b和a，因为tag[0]的排序最低，其次是[1]，再其次是[3]。

10 非典型编码规则

非典型编码规则使用的数据值的编码是第8章描述的基本编码及下列的限制，这些限制也在第11

章中列出。

10.1 长度形式

应使用确定长度编码形式，用最小数目的八位位组进行编码［与 8.1.3.2 b)对比］。

10.2 串编码形式

对位串、八位位组串和受限字符串类型，应不使用结构化编码的形式(与 8.21.6 对比)。

10.3 集合成分

集合值的成分值的编码应按照 GB/T 16262.1—2006 中的 8.6 中规定的标签所确定的次序出现。

注：当集合的成分是无标签的选择类型时，该成分在次序中的位置将依赖于要编码的选择成分的标签。

11 CER 和 DER 使用 BER 的限制

在第 8 章及其各条对“应是 BER 编码”的引用应解释为“适当时，应是 CER 或 DER 编码”(见 8.16.1、8.17.1、8.18.1 和 8.22.1)。

11.1 布尔值

如果编码表示布尔值 TRUE，则其单个内容八位位组应使所有 8 位都置 1(与 8.2.2 对比)。

11.2 未使用的位

11.2.1 位串值编码的最后 1 个八位位组的各个未使用的位应置 0。

11.2.2 在应用 GB/T 16262.1—2006 中的 21.7 时，应在编码位串之前除去所有尾 0 位。

注 1：在使用大小限制的情况下，解码器交付给应用的抽象值是那些满足该大小约束的抽象值之一，并且仅仅不同于用若干尾 0 位发送的值。

注 2：如果位串值没有置 1 的位，那么，编码器应编码长度为 1 和初始八位位组置 0 的值。

11.3 实数值

11.3.1 如果编码表示基数 B 是 2 的实数值，则应使用利用基数 2 的二进制编码。在编码之前，选定尾数 M 和指数 E，使 M 是 0 或奇数。

注：这是必要的，因为若 $M \neq M'$，同一个实数值可以看成$\{M,2,E\}$和$\{M',2,E'\}$，对某一非 0 的整数 n：

$$M' = M \times 2^{-n}$$

$$E' = E + n$$

在值的编码中，二进制比例因子 F 应为 0，M 和 E 应分别用必需的最少八位位组表示。

11.3.2 如果编码表示基数 B 为 10 的实数值，则应使用十进制编码。在形成编码时，下列内容适用：

11.3.2.1 应使用 SJ/Z 9047—1987 NR3 形式。

11.3.2.2 编码中应不使用 SPACE。

11.3.2.3 如果实数值是负数，则它应以 MINUS SIGN(−)开始，否则，它应以一个数字开始。

11.3.2.4 尾数的第 1 个和最后 1 个数字都不可以是 0。

11.3.2.5 尾数的最后 1 个数字后应紧跟一个 FULL STOP(.)，再跟一个指数记号 E。

11.3.2.6 如果指数是 0，它应写成“+0”，否则，指数的第 1 个数字不应是 0，也不应使用 PLUS SIGN。

11.4 GeneralString 值

仅当字符的登记项当前不指明为 G0、G1、G2、G3、C0 或 C1 集时，**GeneralString** 类型(及其子类型)值的编码应生成转义序列，以指明和调用新的登记项。所有指明和调用应进入最小编号的 G 或 C 集合，对于 G 或 C 集合来说，存在与转义序列一起要使用的编码字符集的国际登记簿中的项所定义的一个转义序列。

注 1：对于上述条款的目的，G0 是最小编号的 G 集，然后依次是 G1、G2 和 G3。C0 是最小编号的 C 集，随后是 C1。

注 2：字符串值中的每个字符与编码字符集的国际登记簿中的特定项有关联。

11.5 默认值的集合和序列成分

集合值或序列值的编码应不包括等于其默认值的任何成分值的编码。

11.6 单一集合成分

单一集合值的成分值的编码应按升序出现，要被比较的编码八位位组串正如带有较短成分的八位位组串在其尾端用置为0的八位位组来填充那样进行比较。

注：填充的八位位组仅为了比较的目的，在编码中不出现。

11.7 GeneralizedTime(通用时)

11.7.1 编码应按照GB/T 16262.1—2006对GeneralizedTime条所描述的那样，以一个"Z"来终止。

11.7.2 秒元素应总是存在的。

11.7.3 若存在分秒元素，应忽略所有末尾0；若该元素相当于0，则它们应全部被忽略，十进制小数点也应被忽略。

示例

秒元素"26.000"应表示为"26"；

秒元素"26.5200"应表示为"26.52"。

11.7.4 若存在十进制小数点元素，则它应是小数点选项"."。

11.7.5 午夜(GMT)应以下列形式表示：

"YYYYMMDD000000Z"

其中，"YYYYMMDD"表示上述午夜之后的一天。

示例

有效表示的示例：

"19920521000000Z"

"19920622123421Z"

"19920722132100.3Z"

无效表示的示例：

"19920520240000Z"(不正确表示的午夜)

"19920622123421.0Z"(假的末尾0)

"19920722132100.30Z"(假的末尾0)

11.8 UTCTime(世界协调时)

11.8.1 编码应按照GB/T 16262.1—2006对UTCTime条所描述的那样，以一个"Z"来终止。

11.8.2 秒元素应总是存在的。

11.8.3 午夜(GMT)应该以下列形式表示：

"YYMMDD000000Z"

其中，"YYMMDD"表示上述午夜之后的一天。

11.8.4 有效表示的示例

"920521000000Z"

"920622123421Z"

"920722132100Z"

11.8.5 无效表示的示例

"920520240000Z"(不正确表示的午夜)

"9207221321Z"("00"秒被忽略)

12 传送语法定义中的BER、CER和DER的使用

12.1 对于单个ASN.1类型的所有值，无论何时需要规定一个无歧义的、不可分割的和自界定的八位位组串的表示，都可以引用和应用本部分规定的编码规则。

注：所有这样的八位位组串在单个ASN.1类型的范围内是无歧义的。若与不同的ASN.1类型的编码相混合，则不一定是无歧义的。

12.2 下列客体标识符和客体描述符的值被赋予用来标识和描述本部分规定的基本编码规则：

{joint-iso-itu-t asn1 (1) basic-encoding (1)}和

"Basic Encoding of a single ASN.1 type"

12.3 下列客体标识符和客体描述符的值被赋予用来标识和描述本部分规定的正则编码规则：

{joint-iso-itu-t asn1(1) ber-derived(2) canonical-encoding(0)}和

"Canonical encoding of a single ASN.1 type"

12.4 下列客体标识符和客体描述符值被赋予用来标识和描述本部分规定的非典型编码规则：

{joint-iso-itu-t asn1(1) ber-derived(2) distinguished-encoding(1)}和

"Distinguished encoding of a single ASN.1 type"

12.5 在无歧义的规范将抽象语法定义为抽象值的集合时，其中每一个就是某一特定命名的 ASN.1 类型的值，通常(但不一定)是选择类型的值，那么，12.2、12.3 或 12.4 中规定的客体标识符的值之一可以与抽象语法名称一起用来分别标识出对应在定义抽象语法时所使用的、特定命名的 ASN.1 类型的基本编码规则、正则编码规则或非典型编码规则。

12.6 在 12.2、12.3 和 12.4 中规定的名字不应与抽象语法名称一起用来标识传送语法，除非满足抽象语法定义用的 12.5 中的条件。

附 录 A
（资料性附录）
编码的示例

本附录通过提出一个用 ASN.1 定义的（假想）人事记录的八位位组表示来说明本部分中的基本编码规则。

A.1 记录结构的 ASN.1 描述

假想的人事记录的结构在下面使用 GB/T 16262.1—2006 中为了定义类型而规定 ASN.1 形式描述。

```
PersonnelRecord ::= [APPLICATION  0] IMPLICIT  SET {
        Name                Name,
        title               [0]  VisibleString,
        number              EmployeeNumber,
        dateOfHire          [1]  Date,
        nameOfSpouse        [2]  Name,
        children            [3]  IMPLICIT
            SEQUENCE OF ChildInformation  DEFAULT {} }
ChildInformation ::= SET
        { name              Name,
          dateOfBirth       [0]  Date}
Name ::= [APPLICATION  1] IMPLICIT  SEQUENCE
        { givenName         VisibleString,
          initial           VisibleString,
          familyName        VisibleString}
EmployeeNumber ::= [APPLICATION  2] IMPLICIT  INTEGER
Date ::= [APPLICATION  3] IMPLICIT  VisibleString -- YYYYMMDD
```

A.2 记录值的 ASN.1 描述

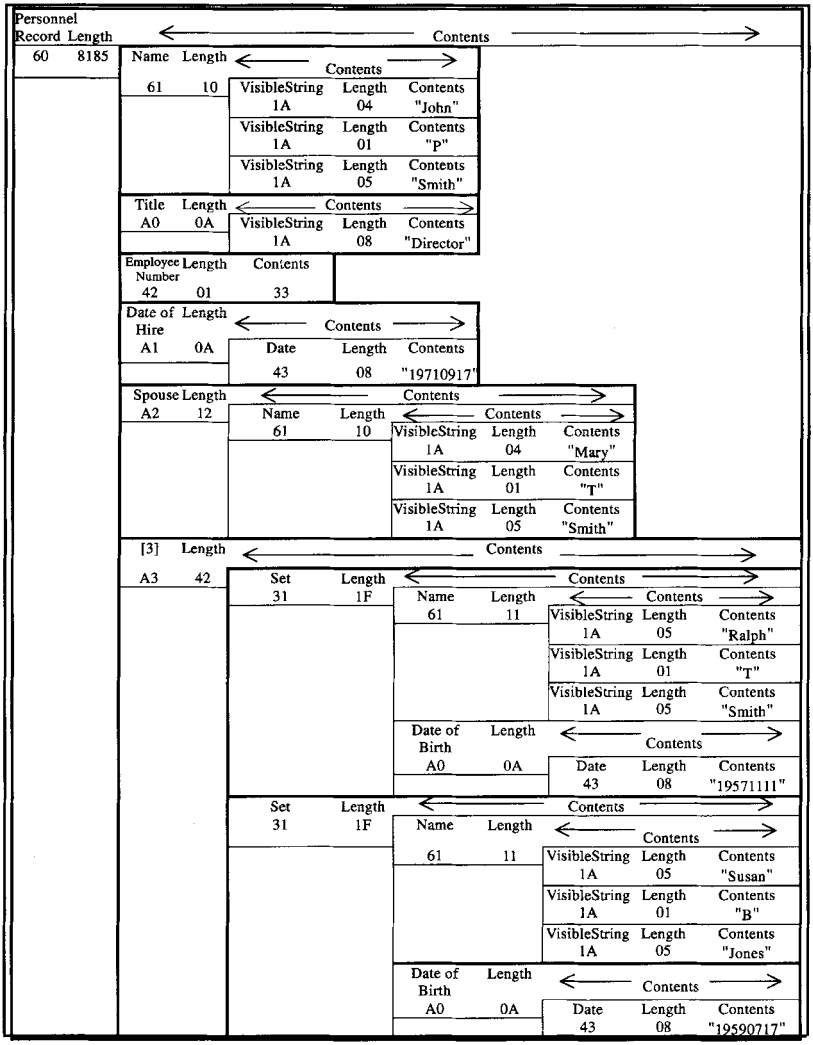
John Smith 的个人记录的值使用 ASN.1 进行形式描述如下：

```
{name  {givenName "John",initial "P",familyName "Smith"},
        title               "Director",
        number              51,
        dateOfHire          "19710917",
        nameOfSpouse        {givenName "Mary",initial "T",familyName "Smith"},
        children
            {
                {name   {givenName "Ralph",initial "T",familyName "Smith"},
                         dateOfBirth "19571111"
                },
                {name   {givenName "Susan",initial "B",familyName "Jones"},
                     dateOfBirth "19590711"
```

```
                    }
                }
        }
```

A.3 该记录值的表示

上面所给的记录值用八位位组的表示如下(应用了本部分定义的基本编码规则后)。标识符、长度和整数的内容八位位组的值用十六进制表示,每个八位位组是二个十六进制数。字符串内容的值的表示为文本,每个八位位组一个字符。


Personnel Record Length
Contents
60 8185
Name Length
Contents
61 10
VisibleString Length Contents
1A 04 "John"
VisibleString Length Contents
1A 01 "P"
VisibleString Length Contents
1A 05 "Smith"
Title Length
Contents
A0 0A
VisibleString Length Contents
1A 08 "Director"
Employee Number Length Contents
42 01 33
Date of Hire Length
Contents
A1 0A
Date Length Contents
43 08 "19710917"
Spouse Length
Contents
A2 12
Name Length
Contents
61 10
VisibleString Length Contents
1A 04 "Mary"
VisibleString Length Contents
1A 01 "T"
VisibleString Length Contents
1A 05 "Smith"
[3] Length
Contents
A3 42
Set Length
Contents
31 1F
Name Length
Contents
61 11
VisibleString Length Contents
1A 05 "Ralph"
VisibleString Length Contents
1A 01 "T"
VisibleString Length Contents
1A 05 "Smith"
Date of Birth Length
Contents
A0 0A
Date Length Contents
43 08 "19571111"
Set Length
Contents
31 1F
Name Length
Contents
61 11
VisibleString Length Contents
1A 05 "Susan"
VisibleString Length Contents
1A 01 "B"
VisibleString Length Contents
1A 05 "Jones"
Date of Birth Length
Contents
A0 0A
Date Length Contents
43 08 "19590717"

附 录 B
（资料性附录）
客体标识符赋值

下列值在本部分中赋值：

条	客体标识符值
12.2	{joint-iso-itu-t asn1 (1) basic-encoding (1)}
	客体描述符值
	"Basic Encoding of a single ASN.1 type"
条	客体标识符值
12.3	{joint-iso-itu-t asn1 (1) ber-derived(2) canonical-encoding(0)}
	客体描述符值
	"Canonical encoding of a single ASN.1 type"
条	客体标识符值
12.4	{joint-iso-itu-t asn1 (1) ber-derived(2) distinguished-encoding(1)}
	客体描述符值
	"Distinguished encoding of a single ASN.1 type"

附 录 C
（资料性附录）
实数值编码的实例

C.1 发送器通常检查自己的硬件浮点表示，以便确定用来传送在该浮点表示与 ASN.1 实数值编码的长度八位位组和内容八位位组之间的值的（依赖于值的）算法。本附录说明了通过使用图 C.1 所示的尾数的（人工）硬件浮点表示在这样的过程中能够采取的步骤。

假设该指数作为一个整数 E 它能容易地从浮点硬件得到。

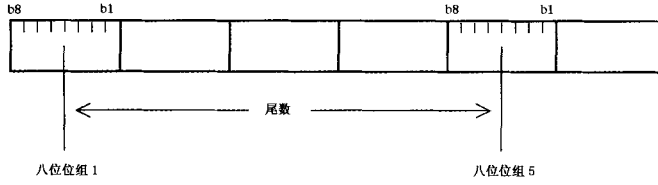


图 C.1 浮点表示

C.2 需要为了发送使用二进制编码的非 0 值（如本部分正文中的规定）而产生的内容八位位组是：

I S bb ff ee E 的八位位组 N 的八位位组

其中 S（尾数符号）依赖于被转换的值，bb 的固定的值（比如 10），以表示基数（本例中假定基数为 16），ff 是如 C.3 的描述计算出的 F 值，ee 是如 C.4 的描述计算出的指数值的固定长度（本附录不处理 E 需要超过 3 个八位位组的情况）。

C.3 在强制第 1 个八位位组的位 8 至位 3 和第 5 个八位位组的位 4 至位 1 为 0 后，该算法将发送作为 N 值的硬件表示的八位位组 1 到 5。假设隐含的十进制小数点被定位在交付 E 值的硬件表示中的八位位组 1 的位 2 和位 1 中间，发送之前通过减去 E 值，其隐含位置能移位到第 5 个八位位组之后的最近的点上。在我们的示例系统中，我们对每个指数的减量能移 4 位（因为我们假定基数为 16），所以 9 的减量将隐含的小数点定位在第 6 个八位位组的位 6 和位 5 中间。这样值 M 是 N 乘以 2^3，以便正确地定位 M 中的小数点（所传送八位位组的 N 中隐含的位置是在第 5 个八位位组的位 1 之后）。这样我们得到关键的参数：

$F=3$（所以 ff 是 11）

指数减量＝9

C.4 指数所需要的长度现在通过求出表示下列值所需要的八位位组的最大数计算出来，

E_{min}——超过量——指数减量

E_{max}——超过量——指数减量

其中，E_{min} 和 E_{max} 是指数表示法的最小和最大整数值，超过量是为了产生真实指数值而需要减去的任何值，指数减量如 C.3 计算出来。假设给出 3 个八位位组的长度。那么 ee 是 10。也假设超过量为 0。

C.5 现在，发送算法是：

a) 对于 ASN.1 类型实数，发送带有标签的基本编码规则标识符八位位组字段；

b) 测试 0，如果测试完成，发送带有值为 0 的 ASN.1 基本编码规则长度字段（无内容八位位组），并结束该算法；

c) 测试并记忆尾数符号，并且如果为负，尾数取反；

d) 传送带有值为 9 的 ASN.1 基本编码规则长度字段，那么：

——若为负　则 11101110；或者

——若为正　则 10101110；

e) 产生并发送有下列指数值的 3 个八位位组：

E-9；

f) 将第 1 个八位位组的位 8 至位 3 和第 5 个八位位组的位 4 至位 1 置为 0，然后发送 5 个八位位组尾数。

C.6 接收算法必须准备处理任何 ASN.1 基本编码，但这里可以直接使用浮点单元。我们按如下内容进行：

a) 检验第 1 个内容八位位组；如果它是 1×101110，我们得到的传输与我们的算法相一致，并且能简单地逆转发送算法。

b) 否则，对字符编码，调用标准字符十进制为浮点的转换软件，并根据应用语义（可能设置硬件浮点能处理的最大和最小数）来处理“SpecialRealValue”。

c) 对二进制传输，将 N 放入浮点单元，如有必要丢弃最低有效位结束处的八位位组，乘以 2^F 和 B^E，如有必要取反。实现者可以发现在特定情况下可能的优化技术，但也可以发现（除了与兼容机的发送相关的优化技术外）对它们进行测试得不偿失。

C.7 上述算法只是实例，当然，实现者将确定他们自己最好的策略。