ICS 35.110
L 79

中华人民共和国国家标准

GB/T 16263.1—XXXX/ISO/IEC 8825-1:2021

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 8825-1:2021，IDT）

（征求意见稿）

（在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1－2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是GB/T 16263在《信息技术　ASN.1编码规则》的第1部分，GB/T 16263已经发布了以下部分：

——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；

——第2部分：紧缩编码规则（PER）规范；

——第4部分：XML编码规则（XER）；

——第5部分：W3C XML模式定义到ASN.1的映射。

本文件代替GB/T 16263.1-2006《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》，与GB/T 16263.1-2006相比，除结构调整和编辑性改动外，主要技术变化如下：

——增加了本文件的缩略语“UTF8”（见4）；

——增加了编码结构的相关规定（见8.1.1.5）；

——更改了实数值为0值编码的有关描述（见8.5.2、8.5.3和8.5.9，2006年版8.5.2和8.5.9）；

——增加了“有前缀类型值的编码”的相关规定（见8.14.1）；

——增加了“OID国际化资源标识符值的编码”、“相对OID国际化资源标识符值的编码”和“TIME类型和有用时间类型值的编码”的相关规定（见8.21、8.22和8.26）；

——增加了“TIME类型和有用时间类型值”转换为规范格式的相关规定（见11.9）；

——增加了“OID国际化资源标识符”用来标识和描述基本编码规则（见12）；

本文件等同采用ISO/IEC 8825-1:2021《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》。

本文件由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本文件起草单位：

本文件主要起草人：

本文件及其所代替文件的历次版本发布情况为：

——1996年首次发布为GB/T 16263-1996，2006年第一次修订；

——本次为第二次修订。

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。

本文件定义了可应用于用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。本文件定义了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，它不构成本文件的组成部分。

附录B总结了在本文件中所产生的客体标识符和OID国际资源标识符值的赋值，它不构成本文件的组成部分。

附录C给出了对编码实数应用基本编码规则的示例，它不构成本文件的组成部分。

GB/T 16263拟由四个部分构成。

——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。

——第2部分：紧缩编码规则（PER）规范。

——第4部分：XML编码规则（XER）。

——第 5 部分：W3C XML 模式定义到 ASN.1 的映射。

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）

1　范围

本文件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，用来标识被传送的数据值。本文件还规定了正则编码规则和非典型编码规则集合，它们将值的编码限制为基本编码规则提供的一种替换编码。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

注：本文件基于GB/T 13000-2010。不能在该标准的更高版本上使用。上述引用应解释为对已确定的标准及其所有已发布的修订和技术勘误的引用。

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

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（ISO/IEC 7498-1:1994,IDT）

GB 13000—2010　信息技术　通用多八位编码字符集（UCS）（ISO/IEC 10646:2003,IDT）

GB/T 16262.1—AAAA　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 8824-1:2021,IDT）

GB/T 16262.2—BBBB　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 8824-2:2021,IDT）

GB/T 16262.3—CCCC　信息技术 抽象语法记法一(ASN.1) 第3部分:约束规范（ISO/IEC 8824-3:2021,IDT）

GB/T 16262.4—DDDD　信息技术 抽象语法记法一(ASN.1) 第4部分:ASN.1规范的参数化（ISO/IEC 8824-4:2021,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（ISO 6093:1985,IDT）

ISO/IEC 2375:2003　信息技术 转义序列和编码字符集的登记规程(Information technology - Procedure for registration of escape sequences and coded character sets)

ISO/IEC 6429:1992　信息技术 编码字符集用的控制功能(Information technology—Control functions for coded character sets)

ISO 结合转义序列使用的编码字符集的国际登记簿

3 术语和定义

GB/T 9387.1和GB/T 16262.1界定的以及下列术语和定义适用于本文件。

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定义无歧义且唯一的编码和值之间一对一映射。

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

数据值编码中表示特定值的那部分，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

动态符合性 dynamic conformance

在通信场合中，要求实现遵守预定行为的声明。

3.6

（数据值的）编码 encoding (of a data value)

用来表示数据值的完整八位位组序列。

3.7

内容结束八位位组 end-of-contents octets

数据值编码的一部分，在其末端出现的，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，用来标识值的类型

注：某些ITU-T建议用术语“数据元素”表示八位位组序列，但在本文件中不使用该术语，因为其他标准中使用该术语表示“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

静态符合性 static conformance

从已定义的特性中实现一组有效特性来支持要求的声明。

3.14

尾0位 trailing 0 bit

位串值最后一个位置的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文件。

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
UTF8 通用转换函数8位（见GB 13000的附录D）

5 记法

本文件引用GB/T 16262.1定义的记法。

6 约定

6.1 本文件使用术语“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 本文件中，八位位组中的位从8至1进行编码，其中位8为“最高有效位”，位1为“最低有效位”。

6.3 本文件中，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，并且每个八位位组位置相同，则两个八位位组串相等。当且仅当以下任一条件成立时，一个八位位组串 S_1 大于另一个八位位组串 S_2：

a) S_1 和 S_2 的每个位置的八位位组直到包含 S_2 中最后一个八位位组都相同，但 S_1 较长；

b) S_1 和 S_2 在一个或多个位置上有不同的八位位组，并且在第一个位置上 S_1 中的八位位组大于 S_2 中的八位位组，将这些八位位组视为无符号二进制数，其中第 n 位的权值为 2^{n-1}。

7 符合性

7.1 动态符合性在第 8 章至第 12 章中规定。

7.2 静态符合性由规定这些编码规则的一个或多个应用的标准来规定。

7.3 根据基本编码规则，发送器可以选择使用替代编码，声称符合基本编码规则的接收器应支持所有替代编码。

注：8.1.3.2 b）和表 3 有这种替代编码的示例。

7.4 正则编码规则或非典型编码规则不允许使用替代编码。

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 数据值的编码应由依次出现的 4 个部分组成：

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 内容结束八位位组仅应在长度八位位组的值要求存在时存在（见 8.1.3）。

8.1.1.3 图 1 为编码结构（原始编码或结构化编码），图 2 为可替换的结构化编码。

图 1 编码结构

图 2　一种替换的结构化编码

8.1.1.4　本文件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：在确定编码时，所有的约束记法可忽略不计，并且忽略 CHOICE、SEQUENCE 和 SET 中的所有可扩充性标记，将扩展认为类型的扩展根。

8.1.1.5　没有为本文件规定的编码规则定义编码指令（见 GB/T 16262.1—AAAA 的 3.8.27）。

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 应编码表示表 1 规定的标签类；

b)　按 8.1.2.5 的规定，位 6 应为 0 或 1；

c)　位 5～位 1 应将标签的编号编码为二进制整数，其中位 5 为最高有效位。

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 所示为带有标签类型的标识符八位位组，该标签的范围为 0～30（包括 0 和 30）。

图 3　标识符八位位组（低标签编号）

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后随一个或多个后继八位位组的前导八位位组。

8.1.2.4.1　前导八位位组应编码如下：

a)　位 8 和位 7 应编码用来表示表 1 列出的标签类；

b)　按 8.1.2.5 的规则，位 6 应为 0 或 1；

c)　位 5～位 1 应编码为 11111_2。

8.1.2.4.2　后继八位位组应对标签的编号进行如下编码：

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～位 1，后随第 2 个后继八位位组的位 7～位 1，依次后随每个更后面的八位位组的位 7～位 1，直到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 给出了一个编号大于 30 的标签类型的标识符八位位组。

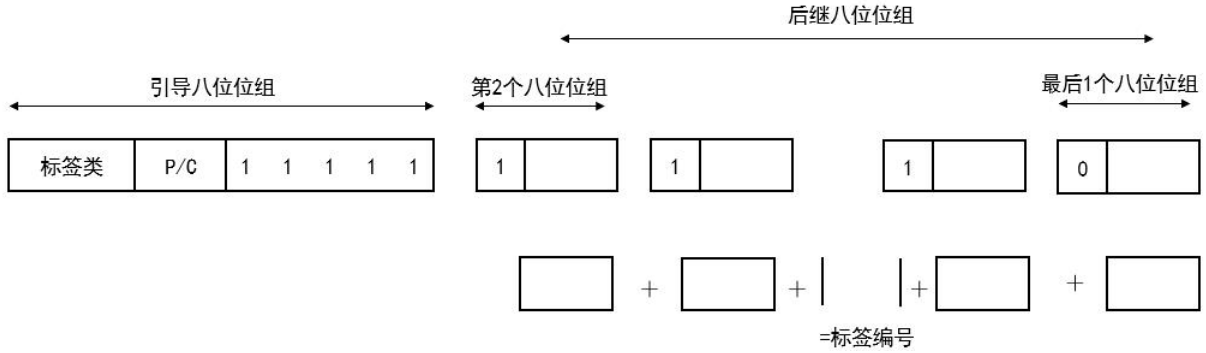


图 4　标识符八位位组（高标签编号）

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，下面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 规定，使用关键字 CHOICE 定义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 16262.1—AAAA 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。该类型随后被定义为 ASN.1 类型，然后其完整编码与所赋类型的值的完整编码相同（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）；

b) 不定形式（见 8.1.3.6）。

8.1.3.2 发送器编码应遵守：

a) 如果是原始编码，则应使用确定形式（见 8.1.3.3）；

b) 如果是结构化编码且都是立即可用的，发送器可以选择使用确定形式（见 8.1.3.3）或不定形式（见 8.1.3.6）作为选项。

c) 如果是结构化编码且不都是立即可用的，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，并且应该表示内容八位位组中的八位位组数，发送器可以选择使用短形式（见 8.1.3.4）或长形式（见 8.1.3.5）作为选项。

注：若内容八位位组中的八位位组个数小于或等于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～位 1 把内容八位位组（它们可能是 0）中的八位位组个数编码为无符号二进制整数，以位 7 为最高有效位。

示例：L=38 的编码为 001001102

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～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) 不应使用值 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～位1，后随第2个后继八位位组的位8～位1，依次后随更后面八位位组的位8～位1，直至最后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。

示例：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，长度八位位组应由单个八位位组组成，表示内容八位位组，并以内容结束八位位组结束（见 8.1.5）。

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末尾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，并应按照后面条款的规定对数据值进行编码。

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

如果长度按照8.1.3.6中规定的方式编码，则应出现内容结束八位位组，否则不应该出现。

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以认为是一个值的编码，该值的标签为通用类，类型为原始编码，标签编号为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，内容八位位组应由单个八位位组组成。

8.2.2 如果布尔值是 FALSE，则八位位组应为 0。

如果布尔值是TRUE，则八位位组应为任意非0值，作为发送器的一个选项。

示例：如果是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 如果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；

b) 应不全为 0。

注：这些规则确保整数值总是用尽可能少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两位二进制补码数，其组成是由第 1 个八位位组的位 8～位 1，后随第 2 个八位位组的位 8～位 1，依次后随每个八位位组的位 8～位 1，直到内容八位位组的最后 1 个八位位组。

注：两位补码二进制数的值是通过对内容八位位组中的位进行编号得出的：从最后1个八位位组的位1开始作为位0，以第1个八位位组的位8结束，每个位被分配一个2^N的数值，其中N是该位在上述编号序列中的位置。这两个补码二进制数的值是通过累加那些值为1的位的数值的和得到的，但不包括第1个八位位组的位8，然后，如果第1个八位位组的位8的值为1，则这个累加值减去第1个八位位组的位8的值。

8.4 枚举值的编码

枚举值的编码应是与其关联的整数值的编码。

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 如果实数值为正 0 值，则编码中应没有内容八位位组。

8.5.3 如果实数值为负 0 值，则应按 8.5.9 中规定的方式进行编码。

8.5.4 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，具体选择是发送器的一个选项。

8.5.5 如果实数值为非 0 值，那么用于编码的基数应为 8.5.4 规定的B'。如果B'是 2、8 或 16，应使用 8.5.7 规定的二进制编码。如果B'是 10，则应使用 8.5.8 规定的字符编码。

8.5.6 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 8.5.7 规定的二进制编码；

b) 如果位 8=0，且位 7=0，则使用 8.5.8 规定的十进制编码；

c) 如果位 8=0，且位 7=1，则按 8.5.9 的规定编码一个“SpecialRealValue”（见 GB/T 16262.1）。

8.5.7 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，例如：

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

$$0 \leq F < 4$$

$$S = +1 \text{ 或 } -1$$

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，为了将隐含的小数点移动到所需的位置，可能要求二进制比例因子F的值不为0。

8.5.7.1 如果 S 为-1，第 1 个内容八位位组的位 7 应为 1，否则为 0。

8.5.7.2 第 1 个内容八位位组的位 6～位 5 决定了编码基数B'的值，具体如下：

位6～位5	基数
0 0	基数为2
0 1	基数为8
1 0	基数为16
1 1	为本文件将来版本保留

8.5.7.3 第 1 个内容八位位组的位 4～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。

8.5.7.4 第 1 个内容八位位组的位 2～位 1 应该编码指数的格式，如下：

a) 如果位 2～位 1 为 00，那么第 2 个内容八位位组将指数的值编码为 2 的补码二进制数；

b) 如果位 2～位 1 为 01，那么第 2 个和第 3 个内容八位位组将指数的值编码为 2 的补码二进制数；

c) 如果位 2～位 1 为 10，那么第 2、第 3 和第 4 个内容八位位组将指数的值编码为 2 的补码二进制数；

d) 如果位 2～位 1 为 11，那么第 2 个内容八位位组编码八位位组的数，例如 *X*（为无符号二进制数）用于编码指数的值，并且第 3 个到第（*X*加 3）个（包括二者）内容八位位组将指数的值编码为 2 的补码二进制数，*X*的值应至少为 1，发送指数的最前 9 位不应全为 0 或全为 1。

8.5.7.5 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，不需要对尾数进行浮点常规化。这允许实现者发送包含尾数的八位位组，但不需要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，进行了常规化的规定，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：实数的这种表示方式与浮点硬件中通常使用的格式有很大不同，但设计的很容易与这种格式进行转换（见附录 C）。

8.5.8 当使用十进制编码时（位 8 至位 7=00），按 SJ/Z 9047 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长度字段，并且按照 SJ/Z 9047 进行编码。SJ/Z 9047 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，具体如下：

位6～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～位1中剩余的值为本文件保留。

不应使用随附文件中规定的比例因子（见 SJ/Z 9047）。

注 1：在 SJ/Z 9047 中关于在小数点前至少使用一个数字的建议，在本文件中也建议这么做，但并不是强制的。

注 2：使用常规化形式（见 SJ/Z 9047）是发送器的一个选项，这不是必须的。

8.5.9 当“SpecialRealValues”或负 0 被编码（位 8～位 7=01）时，应只有一个内容八位位组，具体值如下：

01000000	值为PLUS-INFINITY
01000001	值为MINUS-INFINITY
01000010	值为NOT-A-NUMBER
01000011	值为minus zero

位8～位7等于0和1的所有其他值分别为本文件的补篇保留。

8.6 位串值的编码

8.6.1 位串值的编码应是原始编码，还是结构化编码，作为发送器的一个选项。

注：如果需要在整个位串可用之前传输位串的一部分，则使用结构化编码。

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束位的位串值中的所有位，应从第 1 个后继八位位组的位 8～位 1，第 2 个后继八位位组的位 8～位 1，依次完成每个八位位组的位 8～位 1 的编码，直至最后 1 个后继八位位组需要编码的各个位。

注：术语“引导位”和“结尾位”在GB/T 16262.1—AAAA的22.2中定义。

8.6.2.2 初始八位位组应编码为一个无符号二进制整数，其中位 1 位最低有效位，表示最后 1 个后继八位位组中未使用的位数，该数的范围应为 0～7。

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—AAAA 中的 22.7 时，BER 编码器/解码器可以增加或者删去尾 0 位。

注：如果一个位串值没有1位，那么编码器（作为发送器的选项）可以将该值编码为长度为1，初始八位位组设置为0，或者将它编码为在初始八位位组后有一个或多个0位的位串。

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 用这种方法编码一个八位位组串值时，要将其分段，每个段应由该值的一系列连续位组成，除最后一段外，位数应是 8 的整数倍，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：段的长度可能是0，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，该编码是由本节的递归应用产生的。在该递归应用中，每个段都被视为一个位串值，段的编码应该按照它们的位在整体值中出现的顺序编码到内容八位位组中。

注1：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，作为该递归的结果通常这样的编码是原始编码。

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

类型是BIT STRING的值‘0A3B5F291CD’H可编码如下，在该示例中，位串表示的是原始编码。

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

上面显示出的值也可以按如下进行编码，在该示例中，位串表示的是结构化编码。

位串	长度	内容				
23_{16}	80_{16}	位串	长度	内容		
		03_{16}	03_{16}	$00A3B_{16}$		
		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，并作为发送器的选项。

注：如果需要在整个八位位组串可用之前传输部分八位位组串，则使用结构化编码。

8.7.2 原始编码包含 0 个、1 个或多个内容八位位组，其值与数据值中八位位组的值相等，顺序与他们在数据值中出现的顺序一致，并且数据值的八位位组的最高有效位与内容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 用这种方法编码一个八位位组串值时，要将其分段，每段应由该值的一系列连续八位位组组成，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，该编码是由本节的递归应用产生的。在该递归应用中，每个段都被视为一个八位位组串值。段的编码应该按照它们的位在整体值中出现的顺序编码到内容八位位组中。

注1：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，作为该递归的结果通常这样的编码是原始编码。

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 内容八位位组不应包含任何八位位组。

注：长度八位位组为0。

示例：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 对于带有关键字 OPTIONA 或 DEFAUL 的引用类型，其数据值的编码可以出现，但不是必要的。若数据值编码出现，则其编码应按 ASN.1 定义的类型在相应点上出现。

示例：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 对于带有关键字 OPTIONAL 或 DEFAULT 的引用类型，其数据值的编码可以出现，但不是必要的。

注：集合值中的数据值的次序不重要，对传输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。

8.12.2 同 8.10.2。

8.12.3 编码及后续解码时，不必保持数据值原有的次序。

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 有前缀类型值的编码

8.14.1 如果前缀类型是“EncodingPrefixedType”，则编码是“EncodingPrefixedType”中的“type”，如果前缀类型是“TaggedType”，则适用以下条款。

8.14.2 对于带标签值的编码，应由 8.14.3 和 8.14.4 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。

8.14.3 若类型定义中未使用隐式的标签（见 GB/T 16262.1—AAAA 的 31.2.7），则编码应是结构化编码，且内容八位位组应是完整的基编码。

8.14.4 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，否则为原始编码；

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，这种值的编码在此应为被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“InstanceOfType”记法中使用的特定“DefinedObject-Class”所取代。

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 中的序列类型的组件值应与 GB/T 16262.2—BBBB 的 C.7 中相关类型的对应组件的值相同。

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—AAAA 的 36.5 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—AAAA 中的 36.3a）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 假设外部类型值的编码定义在 EXPLICIT TAGS 环境中，其值应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，即在 GB/T 16262.1—AAAA 的 36.5 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，上述 data-value-descriptor 应出现，并且应有相同的值。

8.18.4 上述 direct-reference 和 indirect-reference 的值是否存在应依照表 2。表 2 把 GB/T 16262.1—AAAA 中 36.5 定义的外部类型替换的标识映射成 18.8.1 中定义的外部类型组件的 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
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编码选择的替换方案中。

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文件中规定的编码规则之一，则发送实现应选择使用下列**编码**选项：

— single-ASN1-type；

— octet-aligned；

— arbitrary。

作为一个实施选项。

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，则发送实现应选择使用下列**编码**选项：

— octet-aligned；

— arbitrary。

作为一个实施选项。

注：如果数据值是一系列ASN.1类型，并且传输语法规定了对每个ASN.1类型应用ASN.1基本编码规则产生的八位位组串的简单连接，则数据值属于此类别，而不是8.18.6。

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：

— arbitrary。

8.18.9 如果**编码**方式选择 single-ASN1-type，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：开放类型中可能出现的值的范围由与direct-reference相关联的客体标识符值的注册和/或与indirect-reference相关联的整数值决定。

8.18.10 如果**编码**方式选择 octet-aligned，那么数据值应按照商定的或协商的编码传输语法进行编码，生成的八位位组应形成八位位组串的值。

8.18.11 如果**编码**方式选择 arbitrary，那么数据值应按照商定的或协商的编码传输语法进行编码，生成的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 内容八位位组应是连接在一起的子标识符（见 8.19.3 和 8.19.4）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共同编码子标识符。在概念上，这些位被连接起来，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，子标识符应用尽可能少的八位位组来编码，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组件的编号少 1。

8.19.4 第 1 个子标识符的数值是从被编码的客体标识符值中的前两个客体标识符组件的值导出来的，使用公式：

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

其中：X是第1个客体标识符组件的值，Y是第2个客体标识符组件的值。

注：前两个客体标识符组件的组合可以识别从根节点只分配了三个值，且从X=0和X=1到达的结点最多分配39个后继值。

8.19.5 第i个子标识符（$2 \leq i \leq N$）的数值是第$(i+1)$个客体标识符组件的数值。

示例：OBJECT IDENTIFIER的值

{joint-iso-itu-t 999 3}

它与下式相同：

{2 999 3}

其第1个子标识符为1079，第2个子标识符为3，所得到的编码为：

OBJECT IDENTIFIER	Length	Contents
06_{16}	03_{16}	883703_{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组件的编码与客体标识符中组件（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 内容八位位组应是连接在一起的子标识符（见 8.20.3 和 8.20.4）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，这些位的组被连接起来，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。子标识符应用尽可能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客体标识符的编号。

8.20.4 第i个子标识符（$1 \leq i \leq N$）的数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 OID 国际化资源标识符值的编码

8.21.1 OID 国际化资源标识符值的编码应是原始编码。

8.21.2 对于 OID 国际化资源标识符类型，内容八位位组应为 XML 值记法（见 GB/T 16262.1—AAAA 的 34.3）中词项字符的 UTF8 编码（见 GB 13000 的附录 D），词项编码之间没有空格。不应使用宣布符和转义序列，每个字符应以该字符可用的最小八位位组数进行编码。

8.22 相对 OID 国际化资源标识符值的编码

8.22.1 相对 OID 国际化资源标识符值的编码应是原始编码。

8.22.2 对于相对 OID 国际化资源标识符类型，内容八位位组应为 XML 值记法（见 GB/T 16262.1—AAAA 的 35.3）中词项字符的 UTF8 编码，词项编码之间没有空格。

8.23 受限字符串类型值的编码

8.23.1 数据值由 ASN.1 类型定义中规定的字符集中的一系列字符串组成。

8.23.2 每个数据值应独立于同一类型的其他数据值进行编码。

8.23.3 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是赋予给GB/T 16262.1中的字符串类型的通用类标签编号，八位位组串的值在8.23.4和8.23.5中规定。

8.23.4 若一个字符串类型在 GB/T 16262.1 中是通过直接引用一个枚举表（NumericString 和 PrintableString）来规定的，则八位位组串的值应是在 8.23.5 中具有相同字符串值的 VisibleString 类型规定的值。

8.23.5 对于除 UniversalString、UTF8String 和 BMPString 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，使用根据 ISO/IEC 2375 登记的转义序列和字符编码。

8.23.5.1 除非是在 GB/T 16262.1 中规定的用来定义字符串类型的登记号之一的转义序列，否则不应使用转义序列。

8.23.5.2 在每串的开始处，某些登记号应被假定指明为 G0 和/或 C0 和/或 C1，且被调用（使用 GB/T 2311 的术语），表 3 对每个类型以及它们隐式的假定的转义序列进行了规定。

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

表 3　转义序列的使用（续）

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
VisibleString （ISO646String）	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：许多常用的字符（例如A到Z）在不同的字符集中出现，每个字符集都有各自的登记号和转义序列。当ASN.1类型允许转义序列时，对一个特定的字符串可能存在多种编码（见7.3）。				

8.23.5.3　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，8.23.5.1 允许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 列出允许有显式转义序列的类型。

8.23.5.4

8.23.5.5　不应使用宣布符，除非 ASN.1 用户明确允许。

注：ASN.1类型的选择还提供了一个宣布符功能的有限形式，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}

8.23.6 上述示例显示了作为发送器选项的三种（更多）可能的有效形式，要求接收器处理所有允许的形式（见 7.3）。

8.23.7 对于 UniversalString 类型，八位位组串应包含在 GB 13000 中规定的使用 4 个八位位组正则形式（见 GB 13000 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 8.23.9 施加的限制，则可以使用该控制功能。

8.23.8 对于 BMPString 类型，八位位组串应包含在 GB 13000 中规定的使用 2 个八位位组 BMP 形式（见 GB 13000 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 8.23.9 施加的限制，则可以使用该控制功能。

8.23.9 在下列例外的情况下，可以使用 ISO/IEC 6429 中的 C0 和 C1 控制功能。

注1：本条的作用是当禁止对其他字符集使用转义时，允许使用有用的控制功能，例如：LF、CR、TAB等。

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

a) 不应使用 GB/T 2311 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。

b) 不应使用 GB/T 2311 中定义的指明或标识转义序列，包括 GB 13000 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也用于选择GB 13000的实现级别，BMPString总是用于选择两个八位位组的形式，UniversalString总是用于选择四个八位位组的形式。

c) 不应使用调用 GB/T 2311 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 13000一致，并保留在该代码集中。

e) 不应使用按照 GB 13000 的 16.3 标识图形字符子集的控制序列。

注5：ASN.1应使用划分子类型来指示GB 13000图形字符的子集，且选择与ISO/IEC 6429控制字符相对应的GB 13000字位。

f) GB 13000 的 16.5 转义序列不应被用于切换为 GB/T 2311 代码。

8.23.10 对于 UTF8String 类型，八位位组串应包含 GB 13000 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。

8.24 无限制字符串类型值的编码

8.24.1 无限制字符串类型值的编码应是 GB/T 16262.1 中 44.5 定义的 BER 类型编码。

8.24.2 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 中的 44.3a））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的值相同。

8.25 有用的类型值的编码

下列这些已经被GB/T 16262.1—AAAA的46至48中给出的定义所替代的“有用的类型”应进行如下编码：

—通用时

—世界协调时

—客体描述符

8.26 TIME 类型和有用时间类型值的编码

8.26.1 TIME 类型值的编码

注：定义的时间类型是TIME类型的子类型，具有相同的标记，并且具有与TIME类型相同的编码。

8.26.1.1 TIME 类型的编码应是原始编码。

8.26.1.2 在删除初始和最后的 QUOTATION MARK(34)字符后，内容八位位组应使用值记法的 UTF-8 编码。

8.26.2 DATE 类型值的编码

8.26.2.1 DATE 类型的编码应是原始编码。

8.26.2.2 在删除首尾 QUOTATION MARK(34)字符以及所有 HYPHEN-MINUS(45)字符后，内容八位位组应使用值记法的 UTF-8 编码。

8.26.3 TIME-OF-DAY 类型值的编码

8.26.3.1 TIME-OF-DAY 类型的编码应是原始编码。

8.26.3.2 在删除首尾 QUOTATION MARK(34)字符以及所有 COLON(45)字符后，内容八位位组应使用值记法的 UTF-8 编码。

8.26.4 DATE-TIME 类型值的编码

8.26.4.1 DATE-TIME 类型的编码应是原始编码。

8.26.4.2 在删除首尾 QUOTATION MARK(34)字符、所有 HYPHEN-MINUS(45)字符、所有 COLON(45)字符以及 LATIN CAPITAL LETTER T 字符后，内容八位位组应使用值记法的 UTF-8 编码。

8.26.5 DURATION 类型值的编码

8.26.5.1 DURATION 类型的编码应是原始编码。

8.26.5.2 在删除首尾 QUOTATION MARK(34)字符以及 LATIN CAPITAL LETTER P 字符后，内容八位位组应是值记法的 UTF-8 编码。

9 正则编码规则

正则编码规则所使用的数据值的编码是第8章中描述的基本编码，加上以下限制以及第11章中列出的限制。

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8.23.6对比），最后一个分片应至少有一个，不超过1000个内容的八位位组。

9.3 集合组件

集合值的组件值的编码应按照GB/T 16262.1—AAAA的8.6中规定的标签指定的顺序出现。此外，为确定组件的编码顺序，当一个或多个组件是无标签的选择类型时，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的标记环境：

```
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
                    }
                }
      }
```

集合组件的编码顺序将总是e、b、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章中描述的基本编码，加上以下限制以及第11章中列出的限制。

10.1 长度形式

应使用确定长度编码形式，用最小数量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，不应使用结构化编码的形式（与8.23.6对比）。

10.3 集合组件

集合值的组件值的编码应按照GB/T 16262.1—AAAA的8.6中规定的标签指定的顺序出现。

注：当集合的组件是无标签的选择类型时，则该组件在排序中的位置将取决于要编码的选择组件的标签。

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8.24.1）。

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—AAAA 的 22.7 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，解码器传递给应用程序的抽象值将是满足该大小约束的抽象值之一，与传输值的不同之处在于尾0位的数量。

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 如果编码表示以 B 为基数 2 的实数值，则应采用以 2 为基数的二进制编码。在编码之前，选则尾数 M 和指数 E，使 M 要么是 0，要么为奇数。

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：

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

$$E' = M + n$$

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 如果编码表示以 B 为基数 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 NR3 形式（见 8.5.8）。

11.3.2.2 编码中不应使用 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

对**GeneralString**类型的值（以及所有其他参考国际编码字符集登记簿定义的受限制的字符串类型）的编码应生成转义序列，仅当字符的登记项当前未被指定为G0、G1、G2、G3、C0或C1集时，才能指定和调用新的登记项。所有的名称和调用都应归入要与转义序列一起使用的编码字符集的国际登记簿的条目中定义的转义序列的最小编号的G或C集合。

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编码字符集登记簿中的特定项有关联。

11.5 默认值的集合和序列组件

集合值或序列值的编码不应包括等于其默认值的任何组件值的编码。

11.6 单一集合组件

单一集合值的组件值的编码应该按升序出现，要被比较的编码八位位组串正如带有较短组件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 中 GeneralizedTime 条描述的那样，以一个“Z”来终止。

11.7.2 秒元素应总是存在。

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 中 UTCTime 条描述的那样，以一个“Z”来终止。

11.8.2 秒元素应总是存在。

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）

11.9 TIME 类型和有用时间类型

11.9.1 TIME、TIME-OF-DAY、DATE、DATE-TIME 和 DURATION 类型的抽象值的值记法应通过以下转换，转换为规范形式：

a) 所有用作十进制符号的逗号都应转换为句号；
b) 所有为整数小时的时差组件的分钟数字应被删除；
c) 如果时间间隔或重复时间间隔包含起点和终点，并且终点包含与起点相同的时差组件，则应删除终点的时差组件；
d) 对于持续时间，以及用起点和持续时间或用持续时间和终点表示的时间间隔中的持续时间（或重复时间间隔中的时间间隔），应修改数值记法，以删除所有零时间组件，但数值记法实例中存在的最不重要的时间组件除外。

11.9.2 对 8.26 中规定的抽象值应该使用所得值记法进行编码。

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文件规定的编码规则。

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、OID 国际化资源标识符（带有 Unicode 标签分配）和客体描述符的值被赋予用来标识和描述本文件规定的基本编码规则：

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

"/ASN.1/Basic-Encoding"

和：

"Basic Encoding of a single ASN.1 type"

12.3 下列客体标识符、OID 国际化资源标识符（带有 Unicode 标签分配）和客体描述符的值被赋予用来标识和描述本文件规定的正则编码规则：

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

"/ASN.1/BER-Derived/Canonical-Encoding"

和：

"Canonical encoding of a single ASN.1 type"

12.4 下列客体标识符、OID 国际化资源标识符（带有 Unicode 标签分配）和客体描述符值被赋予用来标识和描述本文件规定的非典型编码规则：

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

"/ASN.1/BER-Derived/Distinguished-Encoding"

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）
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文件中的基本编码规则。

A.1 记录结构的ASN.1 描述

下面使用GB/T 16262.1规定的用于定义类型的ASN.1正式描述了假定的人事记录的结构。

```
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

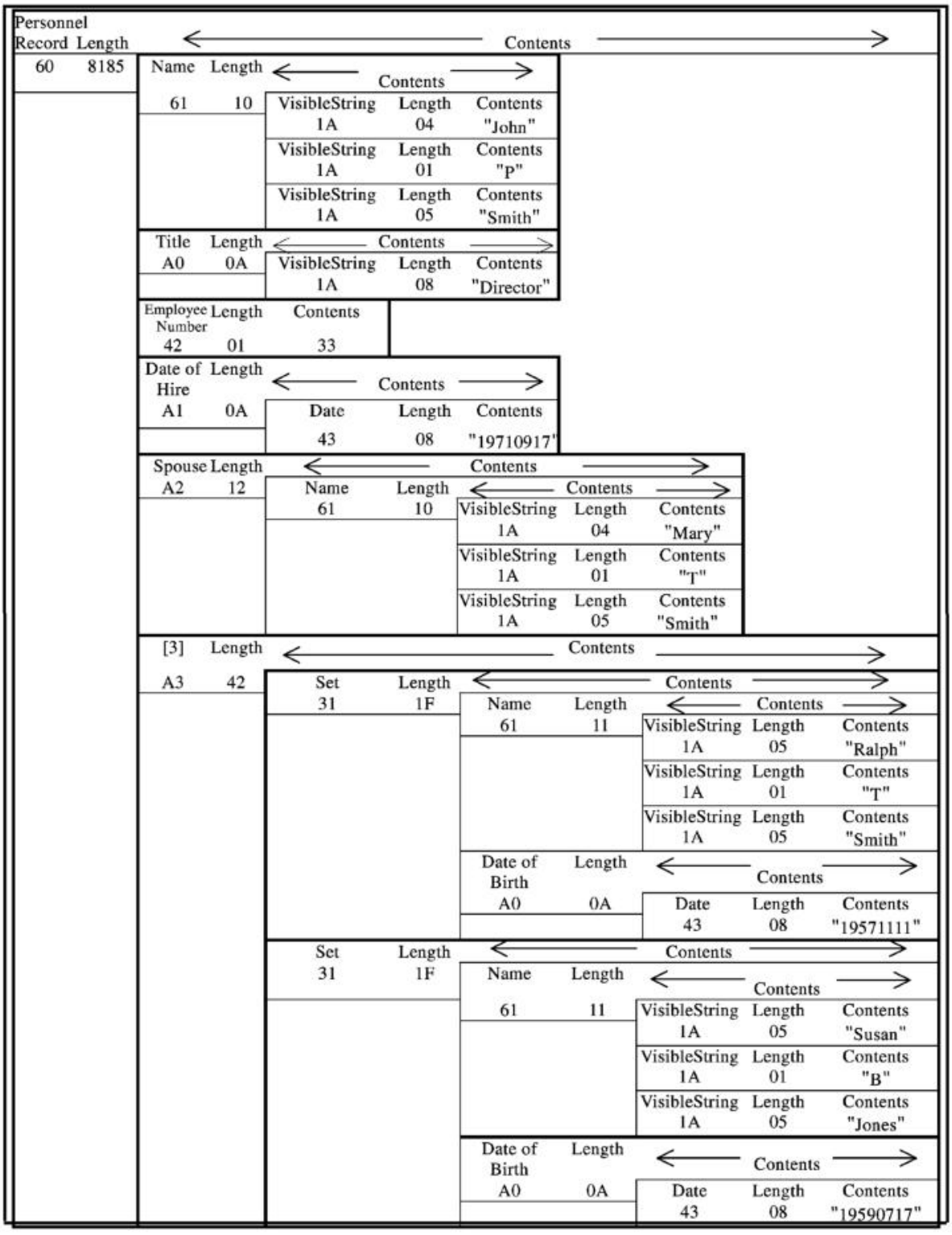
下面使用ASN.1描述了John Smith个人记录的值：

```
{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（应用了本文件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，每个八位位组是两个十六进制数。字符串内容的值表示为文本，每个八位位组表示一个字符。


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

附 录 B
（资料性）
客体标识符赋值

下列客体标识符、OID国际化资源标识符和客体描述符值在本文件中赋值如下：

条 客体标识符值
12.2 {joint-iso-itu-t asn1 (1) basic-encoding (1) }
OID国际化资源标识符值
"/ASN.1/Basic-Encoding"
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) }
OID国际化资源标识符值
"/ASN.1/BER-Derived/Canonical-Encoding"
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) }
OID国际化资源标识符值
"/ASN.1/BER-Derived/Distinguished-Encoding"
客体描述符值
"Distinguished encoding of a single ASN.1 type"

附 录 C
（资料性）
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，以便确定用于在该浮点表示形式与ASN.1 实数值编码的长度和内容八位位组之间传输值的（与值无关的）算法。本附录说明了通过使用图C.1 所示的尾数的（人工）硬件浮点表示在该过程中能够采取的步骤。

假设该指数可以很容易的从浮点硬件中以整数值E的形式得到。

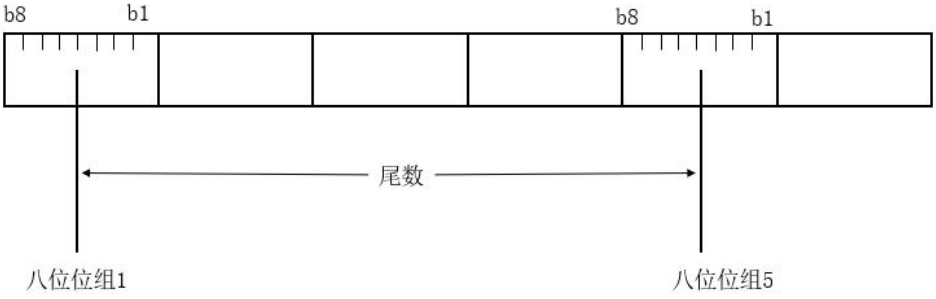


图 C.1 浮点表示

C.2 使用二进制编码（如本文件正文中的规定）发送非零值时需要生成的内容八位位组是：

1 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表示基数（本例中假定基数为16）的固定值，ff是如C.3描述的计算出的固定F值，ee是如C.4描述的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 该算法将硬件表示的八位位组 1 至 5 作为N的值传输，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 强制为零。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，发送之前通过减小E的值，可以将隐含的小数点移动到第 5 个八位位组之后的最近的点上。在我们的示例系统中，我们可以对每个指数的减量移动 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。因此，M的值是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如下：

F=3（所以ff是11）

指数减量=9

C.4 指数所需要的长度现在是通过计算表示下列值所需要的最大八位位组数来计算的：

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中所计算的。假设它的长度是3个八位位组，超过量为0，那么ee是10。

C.5 现在的传输算法是：

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) 测试是否为0，如果是，则发送一个值为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) 测试并记住尾数符号，如果尾数为负数，则取反；

d) 传送值为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) 产生并发送具有下列指数值的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。实施者可能会发现在特定情况下可能的优化技术，但也可能会发现（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，实施者将确定他们自己的最佳策略。