



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

中 华 人 民 共 和 国
国 家 标 准
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

GB/T 16263.1—2006/ISO/IEC 8825-1:2002

*

中 国 标 准 出 版 社 出 版 发 行
北 京 西 城 区 复 兴 门 外 三 里 河 北 街 16 号
邮 政 编 码 : 100045

<http://www.spc.net.cn>

电 话 : (010)51299090、68522006

2006 年 8 月 第 一 版

*

书 号 : 155066 · 1-27836

版 权 专 有 侵 权 必 究
举 报 电 话 : (010)68522006

目 次

| | |
|---------------------------|-----|
| 前言 | III |
| 引言 | IV |
| 1 范围 | 1 |
| 2 规范性引用文件 | 1 |
| 3 术语和定义 | 1 |
| 4 缩略语 | 3 |
| 5 记法 | 3 |
| 6 约定 | 3 |
| 7 一致性 | 3 |
| 8 基本编码结构 | 3 |
| 8.1 编码的一般规则 | 3 |
| 8.2 布尔值的编码 | 6 |
| 8.3 整数值的编码 | 7 |
| 8.4 枚举值的编码 | 7 |
| 8.5 实数值的编码 | 7 |
| 8.6 位串值的编码 | 8 |
| 8.7 八位位组串值的编码 | 9 |
| 8.8 空值的编码 | 10 |
| 8.9 序列值的编码 | 10 |
| 8.10 单一序列值的编码 | 10 |
| 8.11 集合值的编码 | 10 |
| 8.12 单一集合值的编码 | 10 |
| 8.13 选择值的编码 | 11 |
| 8.14 有标签值的编码 | 11 |
| 8.15 开放类型的编码 | 11 |
| 8.16 单一实例值的编码 | 12 |
| 8.17 嵌入式 pdv 类型值的编码 | 12 |
| 8.18 外部类型值的编码 | 12 |
| 8.19 客体标识符值的编码 | 13 |
| 8.20 相关客体标识符值的编码 | 14 |
| 8.21 受限字符串类型值的编码 | 14 |
| 8.22 无限制字符串类型值的编码 | 16 |
| 9 正则编码规则 | 17 |
| 9.1 长度形式 | 17 |
| 9.2 串编码形式 | 17 |
| 9.3 集合成分 | 17 |
| 10 非典型编码规则 | 17 |
| 10.1 长度形式 | 18 |

| | | |
|--------------|----------------------------------|----|
| 10.2 | 串编码形式 | 18 |
| 10.3 | 集合成分 | 18 |
| 11 | CER 和 DER 使用 BER 的限制 | 18 |
| 11.1 | 布尔值 | 18 |
| 11.2 | 未使用的位 | 18 |
| 11.3 | 实数值 | 18 |
| 11.4 | GeneralString 值 | 18 |
| 11.5 | 默认值的集合和序列成分 | 18 |
| 11.6 | 单一集合成分 | 19 |
| 11.7 | GeneralizedTime(通用时) | 19 |
| 11.8 | UTCTime(世界协调时) | 19 |
| 12 | 传送语法定义中的 BER、CER 和 DER 的使用 | 19 |
| 附录 A (资料性附录) | 编码的示例 | 21 |
| 附录 B (资料性附录) | 客体标识符赋值 | 24 |
| 附录 C (资料性附录) | 实数值编码的实例 | 25 |

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。