

文章编号:1001-893X(2011)10-0051-04

一种基于本原多项式的 LDPC 码构建新算法^{*}

蔡 黎¹,代妮娜¹,戴闽鲁^{1,2}

(1.重庆三峡学院 电信学院,重庆 万州 404000;2.日本芝测株式会社,日本 东京 150000)

摘 要:在分析传统 LDPC 编码方式的基础上,提出一种基于本原多项式实现 LDPC 编码的新方法。根据特定 LDPC 码长选择合适的本原多项式作为子矩阵,对子矩阵进行行列分解、组合,最终构建 LDPC 码校验矩阵 H 。仿真实验结果和工程应用证明:新算法构建的 LDPC 码在恶劣的通信环境下,误码率、误帧率优于传统 Mackay-LDPC 码,具有较好的性能。

关键词:LDPC;本原多项式;矩阵分解;校验矩阵

中图分类号:TN911.22 **文献标识码:**A doi:10.3969/j.issn.1001-893x.2011.10.011

A New LDPC Code Construction Algorithm Based on Primitive Polynomial

CAI Li¹, DAI Ni-na¹, DAI Min-lu^{1,2}

(1. Electronic and Information Engineering College, Chongqing Three Gorges University, Wanzhou 404000, China; 2. ShibaSoku Co., Ltd., Tokyo 150000, Japan)

Abstract: A new LDPC (Low Density Parity Check) code constructed by primitive polynomial is proposed based on analysis of traditional LDPC. The appropriate primitive polynomials are selected as the sub-matrixes by the length of the specific LDPC. Then the matrixes are decomposed and combined to construct the check matrix. The simulation and engineering applications prove that the performance of LDPC code constructed by proposed algorithm is better than that of Mackay-LDPC. The BER (Bit Error Rate) and FER (Frame Error Rate) are both lower in the bad communication environment.

Key words: LDPC; primitive polynomial; matrix decomposition; check matrix

1 引 言

低密度校验(LDPC)码是一种性能逼近 Shannon 容量极限的渐进好码,编码性能优越,其长码性能在某些时刻甚至能够超过 Turbo 码^[1],目前已成为 4G 时代重点研究的通信编码方式之一。

本原多项式是一种常见多项式,本质是四环循环编码,因为循环算法的硬件电路实现容易,所以在传统通信编码技术中,经常用到本原多项式编码。

如能将本原多项式循环算法易于硬件实现的优点与 LDPC 码长码时间性能良好的优势相结合,则可能构建一种性能更优的 LDPC 码。因此,本文提出一种基于本原多项式的 LDPC 构建新算法。

2 本原多项式

2.1 本原多项式的定义

一个 n 次不可约的多项式,如能整除 $1 + Z^{2^n - 1}$,

^{*} 收稿日期:2011-06-23;修回日期:2011-08-15
基金项目:重庆市教委科技研究项目(KJ111112);重庆三峡学院青年基金资助项目(10QN-32)
Foundation Item: The Science and Technology Research Program of Chongqing Education Commission (KJ111112); Young Fund Projects of Chongqing Three Gorges University(10QN-32)

而不能整除其它 $1 + Z^l(l, 2^n - 1)$, 可称此不可约多项式为本原多项式^[1]。

设有 2^m 个符号的域为伽罗华域 $GF(2^m)$, 有 2^m 个符号的算法如下: 从有两个符号和一个 m 次多项式 $P(X)$ 开始引入新符号, 若 $P(X) = 0$, 列出 α 的幂的表, 在控制 $P(X)$ 取值的情况下, α 的幂一直到 $2^m - 2$ 都可取得不同值 ($\alpha^{2^m - 1}$ 除外), $0, 1, \alpha, \alpha^2, \dots, \alpha^{2^m - 2}$ 为 2^m 个域元素的集合, 因此, 每个元素可以用 $1, \alpha, \alpha^2, \dots, \alpha^{2^m - 2}$ 之和表示。例如, 当 $m = 4, P(X) = x^4 + x + 1$, 构建如下多项式集合:

$$\begin{aligned} &0 \\ &1 \\ &\alpha \\ &\alpha^2 \\ &\alpha^3 \\ &\alpha^4 = \alpha + 1 \\ &\vdots \\ &\alpha^{12} = \alpha(\alpha^3 + \alpha^2 + \alpha) = \alpha^4 + \alpha^3 + \alpha^2 = \alpha^3 + \alpha^2 + \alpha + 1 \\ &\vdots \\ &\alpha^{15} = \alpha^4 + \alpha = \alpha + \alpha + 1 = 1 \end{aligned}$$

集合中的元素 α 称为域 $GF(2^m)$ 的本原元, 若 $GF(2^m)$ 任一元素的幂能够生成 $GF(2^m)$ 的全部非零元素, 则称它为本原的。

2.2 本原多项式的存在性

综上, 对任意 m 次既约多项式 $P(X)$, 如可给出包含 0 和 1 在内的 2^m 个不同符号的整表, 则称其为本原多项式^[2]。同理, 对于 m 次既约多项式 $P(X)$, 若 $P(\beta) = 0, \beta$ 是 $GF(2)^m$ 的一个本原元素, 则称此多项式是本原多项式。

对于任意正整数 m , 至少存在一个 m 次本原多项式。 m 次本原多项式的存在, 为用其构造 LDPC 码提供了理论依据。

3 本原多项式 LDPC 码的构造

3.1 构造规则

LDPC 码是一种校验矩阵为稀疏矩阵的编码, LDPC 码定义为稀疏奇偶校验矩阵 H 的零空间, 即有 $H * C_T = 0$, 其中 C 是码字序列。

本文提出如下的 H 矩阵的结构构造规则:

- (1) 设 H 矩阵每列含 1 的个数为较小的常数 w_c ($w_c \geq 3$);
- (2) 设 H 矩阵每行含 1 的个数为较小的常数 w_r ($w_r \geq w_c$);
- (3) H 矩阵任何两列之间同为 1 的行数不超过 1, H 矩阵中不含四角为 1 的小方阵, 即无 4 线循环^[3], 最小围线至少是 6;
- (4) w_c 和 w_r 小于码字长度 N , 行数 $M(Nw_c/w_r) \rightarrow \infty$, 则 $w_r/N = w_c/M \rightarrow 0$ 时, 可证明以上规则构造的 H 矩阵是稀疏矩阵。

3.2 构造算法

本原多项式的核心优势是利于循环, 因此本构造算法仍然基于循环原理, 结合矩阵的行列分解技术, 易于硬件实现。具体构造步骤如下所述。

- (1) 根据实际应用系统标准中规定的码长 N 和信息位数 M , 确定校验矩阵 H 的参数: 行数等于 $N - M$, 列数等于 N 。
- (2) 在域 $GF(2^{m-1})$ 上选择合适的本原多项式 $P(X)$ 。本原多项式中系数为 1 的项的个数与矩阵行重 w_r 相等。 m 和 w_r 须满足 $m = N/w_r$, 且都为正整数。因为 m 越大, 在 $GF(2^{m-1})$ 中找寻本原多项式的运算就越复杂, 所以计算时一般将 m 的取值范围控制在约定的范围内, 以尽量减少循环次数。
- (3) 将 $P(X)$ 的向量形式进行 $m - 1$ 次右循环得到 $m \times m$ 的子矩阵 H' , 再进行列分解, 设列分解因子 $t = w_r$, 得到列分解后的 w_r 个 $m \times m$ 矩阵 $H'^i (i = 1, 2, \dots, w_r)$, 对 H'^i 进行列组合得到 $m \times N$ 矩阵 H''_1 。
- (4) 若 $N - M < m$, 则需要重新选择本原多项式; 若 $N - M > m$, 则需要重新选择本原多项式进行行扩展, 此多项式来自伽罗华域 $GF(2^{m_2-1})$, 且 $m_2 < m, m_2 = N - M - m$, 返回到第三步循环; 若 $N - M = m, H''_1$ 即为所求的校验矩阵 H , 结构应如图 1 所示。

H_1^1	H_1^2	$\dots$	$H_1^{w_r}$
H_2^1	H_2^2	$\dots$	$H_2^{w_r}$
$\vdots$	$\vdots$	$\ddots$	$\vdots$

图 1 校验矩阵 H 的结构
Fig.1 Structure of check matrix H

基本算法流程图如图 2 所示。

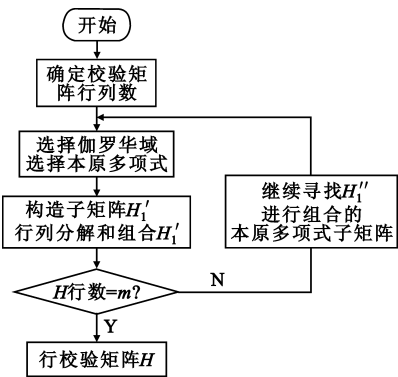


图 2 算法流程图
Fig.2 Algorithm flowchart

3.3 构造实例

设有伽罗华域 $GF(2^7)$ 的本原多项式,表达式为 $P(X) = 1 + X^3 + X^7$,写成 0、1 的序列向量为 (1,0,0,1,0,0,0,1),该向量经过 $m = 7$ 次循环移位得到 8×8 矩阵 H'_7 :

$$H'_7 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

H'_7 校验矩阵的行重、列重为 3,当且仅当列分解因子 $t = 3$ 时,才有 $w_1 = w_2 = w_3 = 1$, H'_7 能分解成 3 个 8×8 的子矩阵,子矩阵行重、列重都为 1。可将分解后的子矩阵看作 3 个单位矩阵的随机变化排列结果,对 H'_7 进行分解,得到新的 8×24 矩阵 H_7 , H_7 行重、列重分别为 3、1。

$$H_7 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

利用检验校验矩阵是否有 4 环的方法进行检验,可得矩阵 H_7 没有 $Girth = 4$ 的环^[4]。

同理,用上述方法也可得到利用其它本原多项式循环矩阵经过分解的子矩阵。多个这样的子矩阵进行组合就可以得到任意行重、列重的规则 LDPC

码校验矩阵^[5]。

在组合得到 LDPC 码校验矩阵的过程中,若选择本原多项式 $P(X) = 1 + X + X^6$ 生成循环矩阵与 H_7 组合,则需对多项式的向量进行填充处理,具体算法是在向量末尾加 0 补充至 8 项,再分解可得七阶本原多项式相似矩阵 H_6 :

$$H_6 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

将 H_6 和 H_7 进行物理组合,得校验矩阵 H :

$$H = \begin{bmatrix} H_6 \\ H_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

显然,组合方法能够将校验矩阵 H 扩展为行重为 3、列重为 2 的稀疏矩阵,矩阵无 $girth = 4$ 的环。

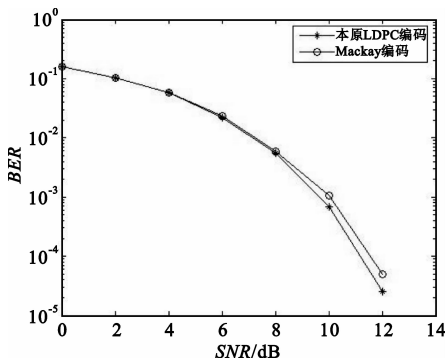
若需增加此校验的行重,则可选取阶数小于 7 的本原多项式进行横向组合,方法与上类似。

4 性能分析

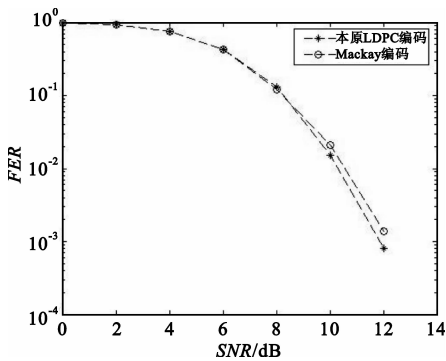
4.1 仿真分析

将码率同为 1/3、矩阵格式为 (16,24,2) 的采用传统 Mackay 算法构建的 Mackay – LDPC 码和用上述算法构造的本原 LDPC 码进行对比仿真实验。

实验采用常用的硬判决译码方式进行译码,在单输入单输出 (Single – input Single – output, SISO) AWGN 信道环境中进行信号传输,主要对比参数为误码率 (BER) 和误帧率 (FER),用 Matalab7.0 仿真得到的结果如图 3 所示。



(a) 误码率性能



(b) 误帧率性能

图 3 本原 LDPC 和 Mackay 码性能比较图
Fig.3 Performace comparison between
primitive - LDPC code and Mackay - LDPC code

观察图 3,以信噪比(SNR)等于 8 dB 为分界线,当 $SNR < 8$ dB 时,本原 LDPC 码与 Mackay - LDPC 码的误码率、误帧率性能相差不大;当 $SNR > 8$ dB 时,本原 LDPC 码的误码率性能、误帧率性能则优于 Mackay - LDPC 码,约大于 0.5 dB。

实验证明:在误码率相同且 SNR 较小环境下,通过新算法得到的基于本原多项式的 LDPC 码性能更优,更能适应恶劣的通信环境。

4.2 工程应用分析

上述算法已经在中国移动多媒体广播 (China Mobile Multimedia Broadcasting, CMMB) 系统中投入工程应用。在实验系统中分别使用本原 LDPC 码和 Mackay - LDPC 码,采用同一计算时间对同一路径路测,统计路测结果文件得到表 1。

表 1 CMMB 系统不同 LDPC 编码路测结果比较
Table 1 Comparison with different LDPC in CMMB

编码	误块率			
	SNR ∈ (0,4]	SNR ∈ [4,8]	SNR ∈ (8,10]	SNR ∈ (10,25]
本原 LDPC	75.4%	30.8%	17.7%	3.0%
Mackay LDPC	77.9%	33.6%	27.0%	7.2%

表 1 说明:当网络覆盖范围小、发射端功率或信号强度正常、满足仿真条件 $SNR < 8$ dB 时,采用两种不同的编码方式得到的通信质量相近;当通信覆盖范围增大、通信环境恶化或发射端输出功率增大,满足仿真条件 $SNR > 8$ dB 时,基于本原多项式的 LDPC 码的通信质量则优于 Mackay - LDPC 码。

实际通信应用与仿真实验结论一致。

5 结 论

(1)新算法能够通过对阶数为 m 的本原多项式进行循环、矩阵分解得到 $(m + 1) \times t(m + 1)$ 的校验矩阵;

(2)仿真和工程应用证明新算法构造方式简单,计算复杂度低,能够在通信恶劣的通信环境中取得较好的质量;

(3)新算法性能真实可靠,已经在 CMMB 系统投入商用,运行稳定。

由于可供选择的本原多项式非唯一,可深入探讨选择最优本原多项式的算法,使其性能进一步提高。

参考文献:

[1] 邓炯.几种 LDPC 码的性能比较[J].电讯技术,2009,49 (5):82 - 85.
DENG Jiong. Performance Comparison for Several Kinds of LDPC Codes[J]. Telecommunication Engineering, 2009, 49 (5):82 - 85. (in Chinese)
[2] Yu Kou, Lin S, Marc P, et al. Low - Density Parity - Check Codes Based on Finite Geometries: A Rediscovery and New Results[J]. IEEE Transactions on Information Theory, 2010, 47(7): 2711 - 2736.
[3] Lan L, Zeng L, Tai Y. Construction of Quasi - Cyclic LDPC Codes for AWGN and Binary Erasure Channels: A Finite Field Approach [J]. IEEE Transactions on Information Theory, 2007, 53(7): 2429 - 2458.
[4] Jun Heo. Analysis of scaling soft information on low density parity check code[J]. Electronics Letters, 2003, 39(1): 325 - 326.
[5] Lan Lan, Yin Yu Tai, Behshad. New Constructions Quasi - cyclic LDPC Codes Based on Special Classes of BIBD's for the AWGN and Binary Erasure Channels[J]. IEEE Transactions on Communications, 2008, 56(1): 39 - 48.

作者简介:

蔡 黎(1981—),男,重庆万州人,2010 年获工学硕士学位,现为讲师,主要研究方向为通信与控制技术;
CAI Li was born in Wanzhou, Chongqing, in 1981. He received the M. S. degree in 2010. He is now a lecturer. His research concerns communication and control technology.
Email: wdjydz@126.com
代妮娜(1983—),女,重庆人,2008 年获工学硕士学位,现为讲师,主要研究方向为通信与信号处理;
DAI Ni - na was born in Chongqing, in 1983. She received the M. S. degree in 2008. She is now a lecturer. Her research direction is communication and signal processing.
戴闽鲁(1954—),男,辽宁沈阳人,1998 年获工学博士学位,现为教授,主要研究方向为无线通信技术。
DAI Min - lu was born in Shenyang, Liaoning Province, in 1954. He received the Ph. D. degree in 1998. He is now a professor. His research direction is wireless communication technology.