带宽有效传输的 GF(q)上 LDPC 编码设计

雷维嘉① 李祥明② 李广军①
①(电子科技大学通信与信息工程学院 成都 610054)
②(重庆邮电学院通信与信息工程学院 重庆 400065)

摘 要：以 Davey(1998)提出的 Monte-Carlo 方法为基础的、适用于二进制 PSK 调制的二进制 LDPC(Low-Density Parity-Check，低密度奇偶校验)码的最优化理论已经在相关文献中得到了验证。但由于 q 进制星座没有旋转对称性，因而限制了 Davey 的方法的应用。本文提出了应用在准正规编码类型上的一种有效的 Davey 型 Monte-Carlo 最优化编码设计方法。应用这种方法，可直接将 GF(q)上的最优 LDPC 编码和任意的 q 进制调制结合起来，获得很高的带宽效率。本文采用 MQAM 和 MPSK 调制机制与准正规 LDPC 编码相结合的若干实例来论证该设计方法。

关键词：低密度奇偶校验(LDPC)码；带宽有效传输；Monte-Carlo 方法
中图分类号：TN911.22 **文献标识码**：A **文章编号**：1009-5896(2007)04-0884-04

Design of LDPC Codes over GF(q) for Bandwidth Efficient Transmission

Lei Wei-jia① Li Xiang-ming② Li Guang-jun①
①(*University of Electronic Science and Technology of China*, *Chengdu* 610054, *China*)
②(*Chongqing University of Posts and Telecommunications*, *Chongqing* 400065, *China*)

Abstract: Optimization of binary LDPC (Low-Density Parity-Check) codes for application to binary PSK modulation has been demonstrated in the literature, on the basis of Monte-Carlo method proposed by Davey(1998). The lack of rotational symmetry in a generic q-ary signal constellation, however, limits the application of Davey's method. This paper proposes an efficient Davey-type Monte Carlo technique for code optimization within the category of quasi-regular codes, so that one can directly combine the optimized LDPC code over GF(q) with arbitrary q-ary modulation to achieve bandwidth efficiency in transmission. The validity of the proposed design procedure is illustrated through examples combining quasi-regular LDPC codes with MQAM and MPSK signaling schemes.

Key words: Low-Density Parity-Check Codes(LDPC); Bandwidth efficient transmission; Monte-Carlo method

1 引言

由于低密度奇偶校验(LDPC)码具有比 Turbo 码等现已实用的编码方法更好的性能，因而近年来重新获得研究人员的重视。随着对高速数据传输的需求不断增加，类似 M 进制 QAM 和 APSK 等的高阶调制技术成为目前的研究热点之一。如何将 LDPC 编码技术与高阶调制技术有机地结合起来，在传输的可靠性和频谱使用的有效性间获得一个很好的平衡就成为一个重要的研究课题。在无线通信系统中由于带宽和信道特性的限制，可靠性和有效性兼顾的问题就显得尤为突出。

最早应用于PSK系统的LDPC编码技术的设计可以追溯到早期Gallager的工作[1]。LDPC编码由稀疏奇偶校验矩阵$\boldsymbol{H}$唯一地确定，编码相对比较简单。根据校验矩阵的行和列的特性，LDPC编码可以分为两大类：正规LDPC编码和非正规LDPC编码。前者要求矩阵所有的行和列具有相同的重量[1]，但后来也允许有不同形式的行重分布$\boldsymbol{r}$和列重分布$\boldsymbol{c}$[2, 3]。设有编码参数 $\Theta=(\boldsymbol{r}, \boldsymbol{c})$，基于该参数可以定义一组稀疏校验矩阵：$\mathcal{H}(\Theta)=\{\boldsymbol{H}: \Theta\}$。从本质上来讲，编码设计的任务就是寻找编码对应的最优的$\mathcal{H}$，使进行可靠传输所需的平均信噪比最小。由于缺少对信噪比函数的显式表达，通过数学的方法来解决这样的最优化问题是很困难的，通常采用Monte-Carlo仿真的办法来解决[2, 3]。Monte-Carlo方法已经在PSK调制的LDPC编码设计中得到了论证[2, 3]。PSK星座具有旋转对称性，这样在Monte-Carlo仿真中就可以选择全零矢量作为LDPC代表码字，从而避免了产生大量由$\mathcal{H}$确定的编码矢量。而对于如MQAM这样使用没有旋转对称性星座的高阶调制，就不能使用全零矢量作为代表码字。对于一般的调制方法，为了使仿真结果能真实地反映$\boldsymbol{H}$的统计特性，就必须产生完整反映星座几何特性的编码符号序列。由于计算的复杂程度太高，实际上这种Monte-Carlo编码设计方法在其星座没有旋转对称性的调制方法中是不可行的。

我们注意到，由于噪声信道的影响，在很多情况下 LDPC 译码器处理的不是 LDPC 的编码码字，而是叠加了错误的矢

2005-09-05 收到，2006-03-13 改回
国家自然科学基金(60572089)，教育部留学回国人员科研启动基金([2005]383)，重庆市自然科学基金(CSTC 2004BB 8602)和重庆市留学回国人员科技活动择优资助项目资助课题

量。LDPC 译码器的工作就是确定这些错误，从接收到的错误序列中恢复出可能性最大的传输码字。受到这个现象的启发，我们提出一种改进的 Monte-Carlo 方法。这种方法中，采用任意矢量和一些附加信息来进行 LDPC 编码的设计，不需要产生 LDPC 编码符号序列。另外，改进的 Monte-Carlo 方法还克服了在将二进制LDPC编码应用于高阶调制时的一个缺点：在发送方进行调制时需要进行比特-符号转换，而在接收方在概率译码前需要进行符号-比特概率转换。改进的方法不需要进行这样的转换，可以直接设计用于 q 进制调制的 GF(q)上 LDPC 编码符号。

本文的第 2 节概要介绍改进的 Monte-Carlo 方法的基本原理，第 3 节介绍该方法的具体实现。该方法在不同调制技术中的应用在第 4 节中介绍，其中提供一些仿真的结果。最后是结束语。

2　基本原理

LDPC 码由其奇偶校验矩阵 $\boldsymbol{H}$ 确定，$\boldsymbol{H}$ 一般采用非系统形式。为了生成确定 Monte-Carlo 优化所需码字矢量的生成矩阵，需要将 $\boldsymbol{H}$ 改写为系统形式，这可采用高斯消元法等方法来实现。用于设计阶段的 $\boldsymbol{H}$ 的维数通常很大，同时运算又是在 GF(q)上进行，这使得计算量非常大。在给定一组矩阵行和列性质的情况下，更是需要确定数百个这样的生成矩阵。因此为编码参数优化直接生成大量的LDPC编码序列显然是不现实的。如果能找到易于生成的等价测试序列来替换这些 LDPC 编码序列，则可以大大降低编码设计的复杂度和运算量。

LDPC 矩阵有两个层次上的功能。首先，当收到符号矢量 $\boldsymbol{x}$ 时，用校验方程 $\boldsymbol{Hx}=\boldsymbol{0}$ 来检查 $\boldsymbol{x}$ 是否是码字。通常情况下，$\boldsymbol{x}$ 由码字 $\boldsymbol{s}$ 加差错矢量 $\boldsymbol{e}$(由信道噪声引起)组成，这样 $\boldsymbol{Hx}$ 的结果将不为零，记这个结果为 $\boldsymbol{a}$，即 $\boldsymbol{Hx}=\boldsymbol{He}=\boldsymbol{a}$。其次，LDPC 矩阵还要确定最稀疏差错矢量 $\boldsymbol{e}$，使发送码字能正确地从接收符号中恢复出来。现假设发送矢量为任意矢量 $\boldsymbol{y}$，$\boldsymbol{Hy}=\boldsymbol{z}$，$\boldsymbol{y}$ 不要求是码字。如果噪声信道产生差错矢量 $\boldsymbol{e}$，则 $\boldsymbol{H}(\boldsymbol{y}+\boldsymbol{e})=\boldsymbol{Hy}+\boldsymbol{He}=\boldsymbol{z}+\boldsymbol{b}$，$\boldsymbol{He}=\boldsymbol{b}$，$\boldsymbol{b}$ 为非零矢量。那么在接收端计算 $\boldsymbol{H}(\boldsymbol{y}+\boldsymbol{e})-\boldsymbol{z}=\boldsymbol{b}$ 与采用真正的 LDPC 码字计算 $\boldsymbol{He}=\boldsymbol{a}$ 在研究 $\boldsymbol{H}$ 的性能上是等效的。LDPC 矩阵设计的关键问题在于其识别差错矢量的能力(性能)，在设计阶段没有必要要求使用真正的码字，($\boldsymbol{y}$, $\boldsymbol{z}$)形式的矢量也可以用来进行 LDPC 编码设计。当 $\boldsymbol{z}=\boldsymbol{0}$ 时，$\boldsymbol{y}$ 就是编码矢量 $\boldsymbol{s}$，因此($\boldsymbol{y}$, $\boldsymbol{z}$)是传统的编码矢量($\boldsymbol{s}$, $\boldsymbol{0}$)的一般形式。使用矢量($\boldsymbol{y}$, $\boldsymbol{z}$)就可以避免设计阶段耗时的码字产生过程。

所有符合给定行和列性质的LDPC矩阵形成一个矩阵集合。以这种方式定义的非正规奇偶校验矩阵集合规模很大，以致在仿真的基础上估计其统计特性变得十分困难。为了在实际应用中可行，希望减小由行和列性质定义的参数空间 Θ，只要求获得次优的 LDPC 编码。可以将研究限制在准正规码的范围内，特别地，考虑只有两个参数构成的参数空间：平均列重 $\overline{w}_c$ 和码率 $R=K/L$，其中 K 和 L 分别为编码前和编码后的长度。而平均行重 $\overline{w}_r$ 可由下式得到

$$\overline{w}_r=\overline{w}_c/(1-R) \tag{1}$$

给定 $\overline{w}_c$ 后，我们使用最简单的准则确定列分布，每列列重可以取两个值：$\lfloor\overline{w}_c\rfloor$ 或 $\lfloor\overline{w}_c\rfloor+1$，称为准正规编码。定义

$$c_j=\begin{cases}\lfloor\overline{w}_c\rfloor-\overline{w}_c+1, & j=\lfloor\overline{w}_c\rfloor\\ \overline{w}_c-\lfloor\overline{w}_c\rfloor, & j=\lfloor\overline{w}_c\rfloor+1\\ 0, & \text{其它}\end{cases} \tag{2}$$

式中 $\lfloor x\rfloor$ 代表实数x的整数部分，$x>0$。c表示校验矩阵$\boldsymbol{H}$中重量为j的列数与总列数之比。同样定义$\boldsymbol{H}$中重量为k的行数与总行数之比r_k

$$r_k=\begin{cases}\lfloor\overline{w}_r\rfloor-\overline{w}_r+1, & k=\lfloor\overline{w}_r\rfloor\\ \overline{w}_r-\lfloor\overline{w}_r\rfloor, & k=\lfloor\overline{w}_r\rfloor+1\\ 0, & \text{其它}\end{cases} \tag{3}$$

从式(1)中可以看到，准正规码可由参数空间Θ=($\overline{w}_c$,R)唯一确定。相应的矩阵集记为 $\boldsymbol{\mathcal{H}}(\Theta)=\{\boldsymbol{H}:\Theta\}$。每个$\boldsymbol{H}$为$M$×$L$维矩阵，其中$M=L$(1–$R$)，其所有元及相关的运算均定义在GF($q$)上。在LDPC编码的理论研究中，主要的工作重点在于研究 $\boldsymbol{\mathcal{H}}(\Theta)$ 的整体性能上，而不是某一个具体的奇偶校验矩阵。对于给定的码率R，我们针对信噪比(SNR) γ 对 $\overline{w}_c$ 进行最优化。用数学符号表示为

$$\overline{w}_{c,\text{opt}}=\arg\min_{\overline{w}_c}\{\gamma(\overline{w}_c)\} \tag{4}$$

由于没有显式的数学表达式，最优化的实现需要采用基于仿真的方法。

通过采用($\boldsymbol{y}$, $\boldsymbol{z}$)形式的矢量和参数空间Θ=($\overline{w}_c$,R) 进行LDPC编码设计，使改进的Monte-Carlo方法运算量和复杂度大大减小，成为可行的方法。在本文随后的部分中将介绍该方法的具体实现。我们用E_b表示传输的平均比特能量，用 γ 或 E_b/N_0(比特能量-噪声比)表示信噪比，BER表示比特误码率。

3　改进的 Monte-Carlo 方法

下面对文献[3]中提出的Monte-Carlo方法进行推广。本文采用一种依赖于后验概率的基于熵的技术来进行译码。先考虑经过AWGN信道传输的接收信号y_i:

$$y_i=s_i+n_i,\quad i=0,1,\cdots,L-1 \tag{5}$$

式中s_i为传输符号，取自q进制星座$\{\alpha_0,\cdots,\alpha_{q-1}\}$。$n_i$为独立复高斯噪声，其分布为$n_i\sim\text{CN}(0,N_0)$。给定接收信号$\{y_0,\cdots,y_{L-1}\}$，需要确定$q$进制星座中每个符号的后验概率。假设现在没有进行编码，而且星座中的每个符号的后验概率都能独立地进行计算。利用贝叶斯公式及所有符号的概率之和为 1 的条件，我们得到

$$\Pr\left(s_i=\alpha_j\left|y_i\right.\right)=\frac{\exp\left(-\left|y_i-\alpha_j\right|^2/N_0\right)}{\sum_{k=0}^{q-1}\exp\left(-\left|y_i-\alpha_k\right|^2/N_0\right)} \tag{6}$$

式中$i=0,1,\cdots,L-1$，$j=0,1,\cdots,q-1$。编码后在$s_i(i=0,1,\cdots,L-1)$间存在约束条件，进行后验概率计算时必须将其考虑进去。设与第i个符号s_i相关联的l个校验方程为$Z_i=\{z_{i1},z_{i2},\cdots,z_{il}\}$。去掉其中任意第$t$个校验方程后为$Z_{i\backslash t}=\{z_{i1},\cdots,z_{i,t-1},z_{i,t+1},\cdots,z_{il}\}$。与文献[3]的表示方法相同，本文用$Q_i^a$表示后验概率$\Pr(s_i=a\mid Z_{i\backslash t})$。式(6)中得到的值通常作为$\{Q_i^a\}$的初始值，用来启动LDPC译码中的和-积算法[1–5]。随后的Q_i^a的值采用和-积算法用迭代的方法得到[3]。

图 1 是基于 Monte-Carlo 仿真的 LDPC 编码最优化的流程图。在给定的数据速率下，对平均列重$\overline{w}_c$进行优化的算法如下：

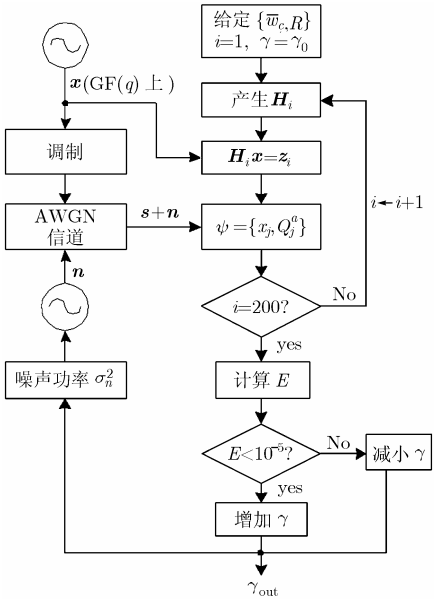

图 1 LDPC 编码设计最优化过程流程图

(1)按均匀分布产生一个L个符号的序列$\boldsymbol{x}=[x_0,x_1,\cdots,x_{L-1}]^{\mathrm{T}}$。这里，$x_j\in\mathrm{GF}(q)$，上标T表示转置。序列的长度$L$很大，在$10^5$数量级上。在调制器中将$\boldsymbol{x}$的每个符号映射到信号星座的信号点上，生成调制矢量$\boldsymbol{s}$。在整个搜索最优的$\overline{w}_c$的过程中，序列$\boldsymbol{x}$和$\boldsymbol{s}$都要用到。

(2)初始化。令i =1，分配初始的E_b/N_0(记作γ_0)给γ，用式(6)的值作为进行平均熵递归计算的初始后验概率值。

(3)为$\overline{w}_c$设定一个值。

(4)随机产生一个校验矩阵$\boldsymbol{H}_i\in\boldsymbol{\mathcal{H}}(\Theta)$。

(5)确定校验方程$\boldsymbol{H}_i\boldsymbol{x}=\boldsymbol{z}_i$。由于$\boldsymbol{H}_i$是稀疏矩阵，因此对于每个元素$x_j$，仅有少量的校验方程与之相联系。存储这些约束条件以供后面使用。

(6)产生高斯白噪声矢量$\boldsymbol{n}$，其方差由γ(即E_b/N_0)确定。

(7)采用文献[3]中的方法，用接收矢量$\boldsymbol{y}=\boldsymbol{s}+\boldsymbol{n}$，信道模型及第(5)步中确定的校验方程一起更新每个x_j的后验概率估计值。

(8)当$i=200$时，用下式计算平均熵：

$$E=-\frac{1}{L}\sum_{i=0}^{L-1}\sum_{a=0}^{q-1}Q_i^a\log_q Q_i^a \tag{7}$$

$E=0$意味着由于噪声信道引起的不确定性已经被完全消除，也就是说发送符号被完整地恢复出来。为减少迭代的次数，迭代的停止条件取为$E=10^{-5}$。如果$E>10^{-5}$，则增加γ，否则减少γ。E_b/N_0增量的选择应使E尽可能快地接近10^{-5}，可以采用Fibonacci或黄金分割法来确定这个增量。更新后的γ用来控制AWGN噪声的方差。$E=10^{-5}$时的γ值称为给定编码参数下的门限SNR。

对于不同的$\overline{w}_c$值，简单地重复第(3)到第(8)步。注意，为使不同$\overline{w}_c$值下得到的门限 SNR 具有可比性，迭代的停止条件应固定。最优的$\overline{w}_c$值时的门限 SNR 是最小的。

4 结果

考虑将GF(q)上的LDPC与q进制调制相结合的情况。设编码长度$L=10^5$，码率$R=0.5$，$q=4$，8 和 16，对应的带宽效率分别为$B=R\log_2 q=1,1.5,2$。对应$q=4$，8，16 的生成伽罗华域GF(q)的本原多项式分别为$p(x)=x^2+x+1$，$p(x)=x^3+x+1$，$p(x)=x^4+x+1$。为简单起见，本文仅考虑准正规LDPC编码，$\overline{w}_c$的优化采用本文第 3 节中介绍的算法。

门限SNR随$\overline{w}_c$变化的情况如图 2 所示。从图中可以看出，对于每个不同的q值，确实存在一个最优的平均列重。从直觉上来看，似乎$\overline{w}_c$越大，门限SNR就越小，这与图中存在一个最优的$\overline{w}_c$值的情况不符。实际上，增大$\overline{w}_c$，意味着对每一个符号将关联更多的校验方程，因而可获得更多的外信息。但如式(1)所示，在给定的编码率R下，增大$\overline{w}_c$也意味着增大$\overline{w}_r$。增大$\overline{w}_r$将使在一个校验方程中涉及到更多的符号。这样，每个符号分享的信息量也就越少，从而导致译码性能的下降。所以，对于给定的R值，$\overline{w}_c$有一个最优的折衷值。

为验证本文的优化过程，选择码长$L=9000$, $R=0.5$，为每个q值选择 3 个$\overline{w}_c$值。对于$q=4$，选择$\overline{w}_c=2.55$，2.75，2.95。其中第 1 个值是最优值，另外两个值较最优值大。同样，$q=8$，选择$\overline{w}_c=2.35$，2.55， 2.75，其中 2.35 是最优值；$q=16$，选择$\overline{w}_c=2.2$，2.4，2.6，其中 2.2 是最优值。$\overline{w}_r$值可用式(1)确定。然后构造校验矩阵$\boldsymbol{H}$和相应的编码生成矩阵。据此可通过计算机仿真得到每个编码调制方法下的误码性能，结果绘制在图 3 中。正如所期望的那样，最优的$\overline{w}_c$值能获得最优的误码性能。3 种编码调制方式GF(4)/QPSK，

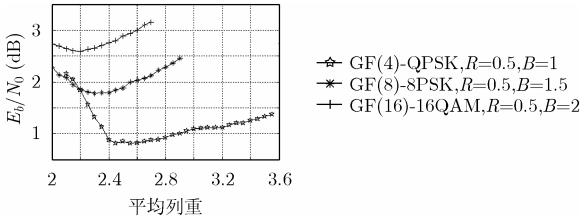

图 2 不同编码调制机制下E_b/N_0与平均列重$\overline{w}_c$关系

GF(8)/8PSK 和 GF(16)/16QAM 均是如此，这也验证了本

文的最优化过程。

在取最优的 $\bar{w}_c$ 值的情况下，研究GF(4)/QPSK、GF(8)/8PSK和GF(16)/16QAM在不同的E_b/N_0下能获得的信道容量是有意义的。3 种机制的带宽效率分别为 1，1.5，2，香农限为$E_b/N_0=0$，0.86，1.76 dB。当编码长度$L=10^5$时，3 种机制可获得的最小E_b/N_0分别为 0.8，1.77，2.59。表 1 中列出了这些值以便比较。一旦获得了每种机制下的最优 $\bar{w}_c$ 值，就可以构造出实用的码长为 9000 的LDPC编码，并通过仿真计算出相应的误码率，如图 3 所示。图中，A，B，C族曲线分别对应 3 种调制机制GF(4)/QPSK，GF(8)/8PSK和GF(16)/16QAM，曲线上方的数据为平均列重，其中每族曲线的最左边一条为最优列重的误码率曲线。从图中可以看出，当误码率为10^{-5} 时，3 种机制要求的E_b/N_0分别为 1.16，2.11，2.91。对于码长达$L=10^5$的情况，3 种机制的性能较香农限差 0.8，0.91，0.83dB。对于可实用的码长$L=9000$，相应的差值为 1.16，1.25，1.15 dB。这说明我们优化的准正规LDPC编码有效地提升了系统性能。

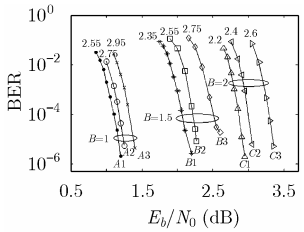

图 3　不同编码调制机制下不同平均列重 $\bar{w}_c$ 对误码率的影响

表 1　3 种LDPC编码/调制机制E_b/N_0(dB)与香农限的比较($(E_b/N_0)_{\text{th}}$表示门限SNR)

	香农限	最小$(E_b/N_0)_{\text{th}}$ $L=100000$	E_b/N_0 BER $=10^{-5}$, $L=9000$
$B=1.0$	0	0.8	1.16
$B=1.5$	0.86	1.77	2.11
$B=2.0$	1.76	2.59	2.91

5　结束语

本文对带宽有效传输中的 GF(q)上 LDPC 编码与 q 进制调制结合起来进行了研究，提出了改进的Monte-Carlo方法。这种方法不需要产生规模巨大的生成矩阵。文中阐述了使用这种方法产生用于加性高斯信道上的QPSK，8PSK和16QAM的最优准正规码的过程。3 种编码/调制机制的带宽效率分别为 1，1.5，2。通过仿真表明该方法能正确地获得最优的平均列重值，用该值来构造LDPC编码时，能够获得很好的误码性能。在 3 种编码调制方式下，在码长$L=9000$ 时，获得BER $=10^{-5}$的性能时所要求的E_b/N_0仅比香农限分别高 1.15～1.25 dB。

参 考 文 献

[1] Gallager R G. Low-Density Parity-Check Codes. Cambridge, Mass., MIT Press, 1963, Chapter 1, 4.

[2] Davey M C and MacKay D J C. Low density parity check codes over GF(q). *IEEE Communications Letters*, 1998, 2(6): 165–167.

[3] Davey M C. Error-correction using low-density parity-check codes. [Ph.D Thesis], University of Cambridge, 1999. http://www.inference.phy.cam.ac.uk/mcdavey/papers/davey_phd.html/

[4] Kschischang F R, Frey B J, and Loeliger H A. Factor graphs and the sum-product algorithm. *IEEE Trans. on Inform. Theory*, 2001, IT–47(2): 498–519.

[5] Li Xiangming and Soleymani M R. A proof of the Hadamard transform decoding of the belief propagation algorithm for LDPCC over GF(q). IEEE Vehicular Technology Conference, VTC2004-Fall, Los Angeles, Sep. 26-29, 2004, Vol. 4: 2518–2519.

雷维嘉：　男，1969年生，高级工程师，研究方向为数字编码和调制技术.

李祥明：　男，1970年生，副教授，博士，研究方向为无线通信技术.

李广军：　男，1950年生，教授，博士生导师，研究方向为通信系统和嵌入式系统设计.