

基于多元 LDPC 码扩展最小和译码的软信息迭代生成算法

何光华^{*①②} 白宝明^{①②} 王雪鹏^①

^①(西安电子科技大学综合业务网理论及关键技术国家重点实验室 西安 710071)

^②(通信网信息传输与分发技术重点实验室 石家庄 050002)

摘要: 为克服多元 LDPC 码的扩展最小和(Extended Min-Sum, EMS)译码算法中对数似然比(Log Likelihood Ratio, LLR)生成及排序复杂度过高的问题, 该文针对以 BPSK 为调制方式的编码调制系统, 提出一种快速而简单的 LLR 生成算法。该算法采用一种低复杂度的迭代计算方式, 可快速生成并排序 LLR, 适用于硬件实现的流水线结构, 能够加速译码器的译码速度并提高译码器吞吐量。仿真结果表明: 所提出算法对译码性能基本没有影响且极大降低 LLR 计算的复杂度, 是一种适用于高速多元 LDPC 译码器前端实现的候选算法。

关键词: 多元 LDPC 码; 有限域; 对数似然比; 软信息; 译码器

中图分类号: TN911.22

文献标识码: A

文章编号: 1009-5896(2011)11-2622-06

DOI: 10.3724/SP.J.1146.2011.00322

An Iterative LLR Derivation Algorithm Based on Extended Min-sum Decoding of Non-binary LDPC Codes

He Guang-hua^{①②} Bai Bao-ming^{①②} Wang Xue-peng^①

^①(State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071, China)

^②(Science and Technology on Information Transmission and Dissemination in Communication Networks Lab, Shijiazhuang 050002, China)

Abstract: To overcome the drawback of the high complexity of Log Likelihood Ratio (LLR) generation and its accompanying sorting in Extended Min-Sum (EMS) decoding of non-binary Low-Density Parity-Check (LDPC) codes, for non-binary LDPC-coded BPSK modulation systems, a high-speed and low-complexity LLR derivation algorithm is proposed in this paper. The proposed algorithm employs an iterative computation method to generate and sort the LLRs. The front-end of a decoder implementing the proposed algorithm can work in pipeline mode, which accelerates the decoding process and increases the throughput of the decoder. Simulation results show that, the proposed algorithm incurs negligible performance loss, which makes it a good candidate for the hardware implementation of the front-end in non-binary LDPC decoders.

Key words: Non-binary LDPC codes; Galois fields; Log Likelihood Ratio (LLR); Soft information; Decoder

1 引言

最早由 Gallager^[1]于 1962 年提出的低密度校验码(Low-Density Parity-Check codes, LDPC codes)被认为是一类逼近香农限的好码。文献[2]首次提出了定义在有限域上的多元 LDPC 码, 他们证实多元 LDPC 码比二元 LDPC 码具有更好的性能, 具体表现在: 能消除四环对译码收敛性的影响, 从而具有更好的纠错性能; 在衰落信道中的抗突发错误能力

更强; 适合较高速率的传输, 即适宜与高阶调制相结合, 从而提供更高的数据传输速率和谱效率^[3,4]。在中、短码长上, 采用 BPSK 调制的等码长条件下, 比二元 LDPC 码具有更好的性能^[5]。在多元 LDPC 码的构造研究上, 文献[6,7]等提出了编码简单、性能较优且具有低错误平层的构造方法。

然而, 多元 LDPC 码的诸多优点却被其高复杂度的译码算法所中和。为降低多元 LDPC 译码复杂度, MacKay 等人^[8]提出一种比 q 元和积译码算法(QSPA)更为简单有效的译码算法, 即基于有限域的快速傅里叶变换和积译码算法(FFT-QSPA)。但对高阶有限域而言, 其运算量仍很巨大。扩展最小和(EMS)译码算法最早由 Declercq 等人^[9]提出, 并后续由 Voicila 等人^[10]对其进行了修正。它是对数似然

2011-04-07 收到, 2011-07-08 改回

国家自然科学基金(60972046, 61001130), 长江学者和创新团队发展计划(IRT0852), 国家科技重大专项基金(2009ZX03003-011, 2010ZX03003-003-03)和通信网信息传输与分发技术重点实验室开放基金(ITU-U1007)资助课题

*通信作者: 何光华 ghhe@mail.xidian.edu.cn

比为度量下的多元和积译码算法的简化，在译码复杂度和译码性能之间做到了很好的平衡，适于硬件的实现^[11,12]，是多元 LDPC 译码器实现的一个较优的候选译码算法。

在采用 EMS 译码算法的多元 LDPC 编码调制系统中，当对 GF(q) 上 LDPC 码字的接收序列进行解调和译码时，并不是将 q 个 LLR 信息全部都利用，而仅仅选取其中 n_m 个最大的 LLR 值。整个 EMS 译码算法的关键一步是 n_m 个最可靠 LLR 的生成以及排序问题。在硬件实现上，由于排序会有很大的译码延迟而造成译码器吞吐量降低，因此针对多元 LDPC 译码器在采用 EMS 译码算法完成硬件实现时，本文提出一种快速有效的 LLR 排序生成算法。

本文的结构如下：第 2 节将介绍多元 LDPC 译码中一些基本定义及 EMS 算法。第 3 节对 EMS 译码算法下的 LLR 进行了重新定义，提出一种基于译码符号硬判决的 LLR 定义，并给出 LLR 的计算公式。第 4 节将介绍所提出的 LLR 迭代排序生成算法。第 5 节将对所提出的算法进行性能仿真和复杂度分析。最后给出全文结论。

2 多元 LDPC 码及 EMS 算法

令 GF(q), q=2^p, 表示一个特征为 2 的有限域, p 为整数。定义在 GF(q) 上码长为 N 的 q 元 LDPC 码 C 可由一个 M×N 的稀疏校验矩阵 H 给出, H=[h_{i,j}], h_{i,j} ∈ GF(q), 其中 M 是校验方程的个数。令 v=[v₀, v₁, ..., v_{N-1}] 表示 C 中一个码字, 则有 vH^T=0。

$$\sum_{j=0}^{N-1} h_{i,j} v_j = 0, \quad i = 0, 1, \dots, M-1 \quad (1)$$

式(1)中所有乘法和加法运算均定义在有限域 GF(q) 上。

在图 1 所示的多元 LDPC 因子图中, 变量节点是有限域 GF(q) 上的任一域元素, 变量节点通过校验矩阵所确定的对应关系与校验节点相连。在每次迭代译码过程中, 消息在校验节点和变量节点之间传递, 而二者通过图 1 中所示的边互连。由于码字符号是有限域上的任一符号, 因此在边上传递消息的长度也是 q, 即消息向量所包含的变量数目为 q。设边上传递的消息是长度为 q 的向量, 记为 U。GF(q) 上的域元素可用一个多项式表示, 令向量 U 中的元素用一 p 维张量表示, 记为 U[a₁, a₂, ..., a_p], 其中 a_k ∈ {0,1}。

U[a₁, a₂, ..., a_p] 在因子图中表示与域元素 a 对应的一个消息。在译码过程中, 校验节点和变量节点之间所传递的消息向量 U 所包含消息长度为 q, 分

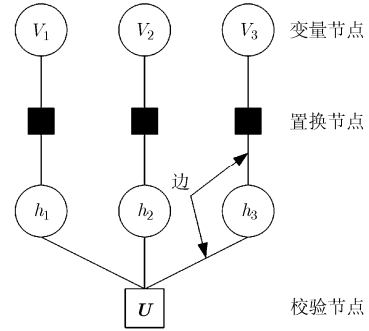


图 1 多元 LDPC 码的校验矩阵中的非零元在因子图中的转换

别对应有有限域 GF(q) 上的 q 个域元素。

EMS 译码算法在迭代译码过程中只传递 q 个消息中置信度较高的 n_m 个消息, 其余消息都以一个常数 γ_A 代替^[10], 其只涉及比较大小和加法运算, 从而降低了计算量。EMS 算法中初始信道消息向量的表示形式为

$$L[a_1, a_2, \dots, a_p] = \log \frac{P(y_i | [c_{i1}, c_{i2}, \dots, c_{ip}] = [a_1, a_2, \dots, a_p])}{P(y_i | [c_{i1}, c_{i2}, \dots, c_{ip}] = [0, 0, \dots, 0])} \quad (2)$$

其中, 每一个对数似然比值为

$$L(x = a_i) = \log \frac{P(x = a_i)}{P(x = 0)} \quad (3)$$

其中 a_i ∈ GF(q), 1 ≤ i ≤ p。

这里要说明: 在迭代译码的过程中, 节点之间所传递的消息向量不仅包含 n_m 个对数似然值, 还需要包含该似然值对应的域元素。

3 基于符号硬判决的 LLR 定义

GF(q=2^p) 上的元素 X 可以表示为一个长度为 p 二进制序列, 即 X=(x₀, x₁, ..., x_{p-1})。在 BPSK 调制下, 令信道接收序列为 Y=(y₀, y₁, ..., y_{p-1}), 则有

$$Y = (y_i = B(x_i) + n_i)_{i=0,1,\dots,p-1} \quad (4)$$

其中 n_i 为加性高斯噪声且 n_i ~ N(0, σ²)。B(x) = 2x - 1, 即判决方式为 B(x) = $\begin{cases} -1, & x = 0 \\ +1, & x = 1 \end{cases}$, 则

ln(P(Y/X)) 可由式(5)得出

$$\begin{aligned} \ln(P(Y/X)) &= \ln \left(\prod_{i=0}^{p-1} P(y_i/x_i) \right) \\ &= p \ln \left(\frac{1}{\sqrt{2\pi\sigma^2}} \right) - \sum_{i=0}^{p-1} \left(\frac{(y_i - B(x_i))^2}{2\sigma^2} \right) \end{aligned} \quad (5)$$

令 Ω 为 GF(q) 上令 ln(P(Y/X)) 具有最大值的域元素。根据式(5), Ω 可以由式(6)得出

$$\Omega = (l_i = \text{HD}(y_i))_{i=0,1,\dots,p-1} \quad (6)$$

其中 HD 表示对 y 进行硬判, 判决方式为

$$\text{HD}(y) = \begin{cases} 0, & \forall y < 0 \\ 1, & \forall y \geq 0 \end{cases}$$

此外, GF(q)中的符号 X 所对应的软信息 $L(X)$ 可由符号 X 的似然概率与 Ω 的似然概率运算得出

$$L(X) = \ln \left(\frac{P(Y/X)}{P(Y/\Omega)} \right) \quad (7)$$

根据式(5), 式(7)可以扩展为

$$\begin{aligned} L(X) &= \sum_{i=0}^{p-1} \ln \left(-\frac{(y_i - B(x_i))^2}{2\sigma^2} + \frac{(y_i - B(l_i))^2}{2\sigma^2} \right) \\ &= -\frac{1}{2\sigma^2} \sum_{i=0}^{p-1} (2y_i (B(l_i) - B(x_i))) \end{aligned} \quad (8)$$

通过定义 Ω , 可以看出 $L(X)$ 是一个负值。为便于计算, 这里定义 $\bar{L}(X) = -L(X)$ 来消除负值在运算中的不便。根据式(7), 可得

$$\bar{L}(X) = \frac{2}{\sigma^2} \sum_{i=0}^{p-1} |y_i| \Delta_i \quad (9)$$

其中 $\Delta_i = x_i \text{ XOR } l_i$, 即

$$\Delta_i = \begin{cases} 0, & \text{当 } x_i \text{ 和 } l_i \text{ 具有相同的符号时} \\ 1, & \text{当 } x_i \text{ 和 } l_i \text{ 具有不同的符号时} \end{cases}$$

下面举例来说明这种 LLR 的定义和计算方法。以 GF(8)上的消息表示方法为例, 在概率域上:

$$\begin{aligned} &P(I = x)_{x \in \text{GF}(q)}, \text{ 其中 } q=8. \\ &(0; \alpha^0; \alpha^1; \alpha^2; \alpha^3; \alpha^4; \alpha^5; \alpha^6) \\ &(0.10; 0.25; 0.05; 0.03; 0.07; 0.04; 0.37; 0.09) \\ &(\sum = 1) \end{aligned}$$

这里可得具有最大似然概率的域元素符号为 α^5 , 令 $hl = \alpha^5$ 。

经典计算 LLR 的方法: $\text{LLR}(x) = \text{LLR}(P(I = x)) - \ln(P(I = 0))$,

$$\begin{aligned} &(0; \alpha^0; \alpha^1; \alpha^2; \alpha^3; \alpha^4; \alpha^5; \alpha^6) \\ &(0; 0.91; -0.69; -1.20; -0.36; -0.92; \\ &1.31; -0.11) \end{aligned}$$

按上文所述, 采用符号硬判决方式的 LLR 计算公式为

$$\text{LLR}(x) = \ln(P(I = x)) - \ln(P(hl)) \quad (10)$$

其中 $P(hl) = 0.37$, 则有

$$\begin{aligned} &(0; \alpha^0; \alpha^1; \alpha^2; \alpha^3; \alpha^4; \alpha^5; \alpha^6) \\ &(-1.31; -0.39; -2.00; -2.51; -1.67; \\ &-2.22; 0; -1.41) \end{aligned}$$

这里可以看出, 得到软信息值都是非正数, 为了避免处理负值带来的不便, 这里重新定义 LLR 为

$$\text{LLR}(x) = \ln(P(I = hl)) - \ln(P(I = x)) \quad (11)$$

则有

$$\begin{aligned} &(0; \alpha^0; \alpha^1; \alpha^2; \alpha^3; \alpha^4; \alpha^5; \alpha^6) \\ &(1.31; 0.39; 2.00; 2.51; 1.67; 2.22; 0; 1.41) \\ &(13; 4; 20; 25; 17; 22; 0; 14) \text{ 采用 6 bit 量化} \end{aligned}$$

(13; 4; 15; 15; 15; 15; 0; 14) 为防止溢出, 进行数值截取。

根据 EMS 译码算法, 若只选取 $n_m=4$ 个最可靠的软信息值, 即

$$L = \{(0, \alpha^5), (4, \alpha^0), (13, 0), (14, \alpha^6)\}$$

用图 2 可以更为直观地了解本文所述的 LLR 生成方法。图 2 所示为 GF(64)域上的发送信号以每符号 6 bit 进行传输。

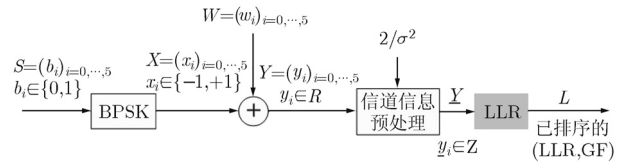


图 2 一个 GF(64)域上的高斯信道传输模型

上述关于 LLR 的重新定义, 针对图 2 可以具体解释为:

设有限域 GF(q)的符号 S 以 6 bit 进行传输, 即 $S = (b_i)_{i=0,1,\dots,5}$, 其中 $b_i \in \{0,1\}$ 。 S 经过 BPSK 调制后映射为 $X = (x_i)_{i=0,1,\dots,5}$, 其中 $x_i \in \{-1,+1\}$, 其判决方式: $x_i = \begin{cases} -1, & b_i = 0 \\ +1, & b_i = 1 \end{cases}$ 。信息序列通过 AWGN

信道所引入的噪声为 $W = (w_i)_{i=0,1,\dots,5}$, 则有 $Y = X + W$, 即 $(y_i)_{i=0,1,\dots,5} = (x_i)_{i=0,1,\dots,5} + (w_i)_{i=0,1,\dots,5}$, 其中 w_i 为加性高斯噪声且 $w_i \sim N(0, \sigma^2)$, 由于引入了噪声, 信息序列将变为实数信号, 即 $y_i \in R$ 。

首先对接收信号 Y 进行硬判决, 根据 $\text{HD} = \text{sign}(Y)$, 有 $\text{LLR}(\text{HD}) = 0$, 则基于符号硬判决的 LLR 定义为

$$L(x) = \ln \left(\frac{P(Y/\text{HD})}{P(Y/X)} \right) = \ln \left(\prod_{i=0}^5 \frac{P(y_i/hl_i)}{P(y_i/x_i)} \right)$$

进一步简化为

$$\begin{aligned} L(x) &= \sum_{i=0}^5 \frac{(hl_i - y_i)^2 - (x_i - y_i)^2}{2\sigma^2} \\ &= \frac{2}{\sigma^2} \sum_{i=0}^5 |y_i| \Delta_i = \sum_{i=0}^5 |y_i| \Delta_i \end{aligned}$$

当 x_i 和 hl_i 具有相同的符号时, $\Delta_i = 0$; 否则, $\Delta_i = 1$ 。

这里可以看出, 软信息 $L(x)$ 的计算公式中存在一个乘数恒因子 $2/\sigma^2$, 为简便起见, 在计算 EMS

译码算法所需置信度最高的 n_m 个 LLRs 之前, 需对接收端所接收到的信息 Y 进行预处理, 预处理将完成 3 个方面的操作: 消除常数恒因子 $2/\sigma^2$, 量化以及数据溢出截断, 目的是使最终得到信息序列 \underline{Y} 是一整数序列, 即 $\underline{Y} = (y_i)_{i=0,1,\dots,5}$, 其中 $y_i \in \mathbb{Z}$, 便于后续进行硬判决及迭代生成排序软信息。

下节将介绍如何快速获得最可靠的 n_m 个 LLRs 及其对应的域元素。

4 LLR 的迭代排序生成算法

本节所要解决的核心问题是要从上一节中所定义的 $\bar{L}(X)$ 中产生 n_m 个最小值, 以及确定它们对应的域元素, 并将其按照实值升序排列。关于 LLR 的排序问题, 最早由 Declercq 等人^[9]提出的 EMS 译码算法以及 Voicila 等人^[10]后续对 EMS 算法进行的改进一文中都提出了解决办法。但是他们所提出的算法在解决排序问题上仍需要很多时钟周期才能完成, 并且耗费大量的存储资源和逻辑资源, 极大限制了采用 EMS 算法的译码器硬件实现。

通过上节中对 LLR 的重新定义, 可以发现: 与传统上对 LLR 进行排序不同的, 本文可按照升序排序对 LLR 进行排序。在译一帧多元 LDPC 码时, 若译码迭代次数不同, 按照本文对 LLR 的定义, 可以省去归一化过程, 使得译码电路更为简单。

本文所提出的 LLR 生成算法是一种迭代构造算法, 在第 s 次迭代时 ($1 \leq s \leq p$)。首先定义 $\bar{L}(X^s) = \frac{2}{\sigma^2} \sum_{i=0}^{s-1} |y_i| \Delta_i$ 为变量 X 的部分 LLR 值。令 ψ_s 表示一个 2 维变量 $(\bar{L}(X^s), X^s)$ 并按照 $\bar{L}(X^s)$ 值的大小对其升序排序。为下文描述方便, 这里 $\bar{L}(X)$ 中的乘数恒因子 $2/\sigma^2$ 暂忽略。

当 $s = 1$ 时,

$$\psi_1^0 = (0, l_0), \psi_1^1 = (|y_0|, \bar{l}_0) \quad (12)$$

即

$$\psi_1 = \{(0, l_0), (|y_0|, \bar{l}_0)\} \quad (13)$$

其中 \bar{l}_0 表示 l_0 逻辑取反。

当 $s = 2$, ψ_2 的生成可由 ψ_1 通过两步递推获得:

第 1 步 将 ψ_1 扩展成两部分 ψ_2^0 和 ψ_2^1 , 这两部分分别对应 $(0, l_1)$ 和 $(|y_0|, \bar{l}_1)$ 。则有

$$\psi_2^0 = \{(0, l_0 l_1), (|y_0|, \bar{l}_0 l_1)\} \quad (14)$$

$$\psi_2^1 = \{(|y_1|, l_0 \bar{l}_1), (|y_0| + |y_1|, \bar{l}_0 \bar{l}_1)\} \quad (15)$$

第 2 步 联合 ψ_2^0 和 ψ_2^1 构造 ψ_2 。

$$\psi_2 = \begin{cases} \{(0, l_0 l_1), (|y_0|, \bar{l}_0 l_1), (|y_1|, l_0 \bar{l}_1), (|y_0| + |y_1|, \bar{l}_0 \bar{l}_1)\}, \\ \quad \forall |y_1| > |y_0| \\ \{(0, l_0 l_1), (|y_1|, l_0 \bar{l}_1), (|y_0|, \bar{l}_0 l_1), (|y_0| + |y_1|, \bar{l}_0 \bar{l}_1)\}, \\ \quad \forall |y_1| \leq |y_0| \end{cases} \quad (16)$$

将上述公式的推导通过递归法扩展到一般情况, 则 ψ_s 的第 k 对变量 $(\bar{L}(X^{s-1})(k), X^{s-1}(k))$ 可由式 (17) 得出

$$\left. \begin{aligned} \psi_s^0 &= (\bar{L}(X^{s-1})(k) + 0, X^{s-1}(k) \& l_s) \\ \psi_s^1 &= (\bar{L}(X^{s-1})(k) + |y_{s-1}|, X^{s-1}(k) \& \bar{l}_s) \end{aligned} \right\} \quad (17)$$

其中 $\&$ 表示二进制符号上的拼接。

综上所述, 若 ψ_s^0 和 ψ_s^1 都已计算得出, 则计算 ψ_s 就变得较简单, 最终通过迭代运算可得 $\psi_s(k) = (\psi_s^0(k), \psi_s^1(k))$ 。由于 EMS 译码算法只需要 n_m 个最小值, 这里 ψ_s 的长度为 2^s 和 n_m 之间的较小值。

下面举一实例详细说明本文所述的 LLR 排序生成过程:

一个 GF(64) 域上的多元 LDPC 编码调制系统, 采用 EMS 译码算法, $n_m = 8$, $p = 4$ 。信道接收值 $Y = (5, -6, -7, 8)$, 则 Y 的硬判决值为 $D = (1, 0, 0, 1)$ 。

当 $s = 1$ 时, 则有

$$\begin{cases} \psi_1^0 = (0, 1) \\ \psi_1^1 = (5, 0) \end{cases} \\ \lambda_1 = \{(0, 1), (5, 0)\}$$

由于 $|y_0| < |y_1|$, 则当 $s = 2$ 时

$$\begin{cases} \psi_2^0 = \{(0, 10), (5, 00)\} \\ \psi_2^1 = \{(6, 11), (11, 01)\} \end{cases} \\ \psi_2 = \{(0, 10), (5, 00), (6, 11), (11, 01)\}$$

依此迭代, 当 $s = 3$ 时,

$$\begin{cases} \psi_3^0 = \{(0, 100), (5, 000), (6, 110), (11, 010)\} \\ \psi_3^1 = \{(7, 101), (12, 101), (13, 111), (18, 011)\} \end{cases} \\ \psi_3 = \{(0, 100), (5, 000), (6, 110), (7, 101), (11, 010), \\ (12, 101), (13, 111), (18, 011)\}$$

最后一次迭代, $s = 4$ 时,

$$\begin{cases} \psi_4^0 = \{(0, 1001), (5, 0001), (6, 1101), (7, 1011), \\ (11, 0101), (12, 1011), (13, 1111), (18, 0111)\} \\ \psi_4^1 = \{(8, 1000), (13, 0000), (14, 1100), (15, 1010), \\ (19, 0100), (20, 1010), (21, 1110), (26, 0110)\} \end{cases} \\ \psi_4 = \begin{cases} \{(0, 1001), (5, 0001), (6, 1101), (7, 1011), (8, 1000), \\ (11, 0101), (12, 1011), (13, 0000), (13, 1111), \\ (14, 1100), (15, 1010), (18, 0111), (19, 0100), \\ (20, 1010), (21, 1110), (26, 0110)\} \end{cases}$$

当 n_m 取值为 8 时, 我们仅从 ψ_4 中选取最小的 8 个值, 即

$$\{(0, 1001), (5, 0001), (6, 1101), (7, 1011), (8, 1000), \\ (11, 0101), (12, 1011), (13, 0000)\}$$

下一节将对所提出算法的性能进行分析和讨论。

5 仿真结果和复杂度分析

本节将对 EMS 译码算法中的采用所提出的 LLR 生成算法和标准 LLR 生成算法下的误比特率 (Bit Error Rate, BER) 和误帧率 (Frame Error Rate, FER) 进行性能比较以及分析在同一译码算法下不同的 LLR 生成算法所需要的复杂度。

例 1 采用一类基于 $GF(q)$ 构造的多元非规则重复累积(QIRA)码^[5]: 所使用的是一个码长为 174 符号, 码率为 1/2 的 $GF(64)$ 上的码字, 其最大行重和列重分别为 6 和 3。调制方式为 BPSK, 采用 AWGN 信道, 最大迭代次数为 50, n_m 取 32。性能仿真如图 3(a) 所示。

例 2 采用一类基于 $GF(q)$ 构造的多元规则 LDPC 码^[13], 所使用的是一个码长为 256 符号, 码率为 1/2 的 $GF(16)$ 上的码字, 其行重和列重分别为 4 和 2。调制方式为 BPSK, 采用 AWGN 信道, 最大迭代次数为 50, n_m 取 8。性能仿真如图 3(b) 所示。

由于本文所提出的 LLR 生成算法仅对 LLR 进行了重新定义, 无任何近似运算, 从信息论的角度, LLR 所表示的含义是等价的, 其性能曲线也应与标准 LLR 生成性相差无几。从图 3 中的性能比较可以印证, 即在采用两类不同构造方法的多元 LDPC 码, 译码算法均为 EMS 译码算法下, 本文所提出的 LLR 迭代排序生成算法与标准 LLR 生成算法的性能基本没有损失。

表 1 给出了 EMS 译码算法下本文所提出的 LLR 的迭代排序生成算法和标准 LLR 标准生成算

表 1 不同 LLR 生成算法所需的译码复杂度比较

LLR 生成算法	实数加法	实数乘法	实数除法	指数运算	比较次数
本文算法	0	0	0	0	$n_m \log n_m$
EMS ^[10]	q	q	q	q	$n_m \log n_m$
FFT-QSPA ^[8]	q	q	q	q	$q \log q$

法, 以及 FFT-QSPA 译码算法中的 LLR 标准生成算法分别在 BPSK 调制下的运算量。

由表 1 可以看出采用 BPSK 调制时, 在 EMS 译码算法下, 采用本文的 LLR 迭代生成算法相对于 LLR 标准生成算法, 虽然每次迭代周期的比较次数相同, 但在实数加法和实数乘法运算得到了很大程度的减少; 而相对 FFT-QSPA 来说, 其每次迭代计算需要的实数加法运算、实数乘法运算量和比较次数均得到了极大的减少。因此在硬件实现上能够为译码器的快速译码节约时间, 降低译码延时并提高吞吐量。

综上所述, 在 EMS 译码算法下, 本文所提出的 LLR 迭代排序生成算法的复杂度比 LLR 标准生成算法和 FFT-QSPA 中的 LLR 生成算法低很多, 并对译码性能的影响可忽略不计。

6 结论

本文提出了一种简单而有效的 LLR 快速生成及排序算法。所提出的算法采用了一种迭代计算方式, 能够快速生成并排序向量对 (LLR, GF)。仿真结果表明, 与标准 LLR 生成排序成算法相比, 本文所提出的 LLR 迭代生成排序算法没有性能损失, 且具有较低的计算复杂度。此外, 本文所提出的算法采用迭代的计算方式, 在硬件实现上可以采用流水线

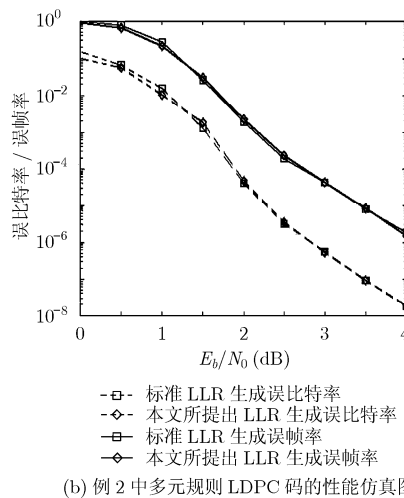
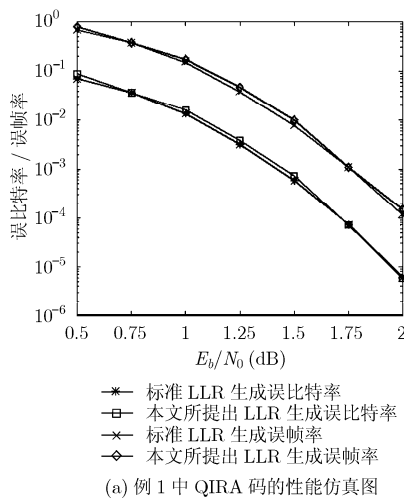


图 3 本文所提出 LLR 生成算法与标准 LLR 生成算法在 EMS 译码算法下 BER/FER 性能对比曲线

结构, 能提高译码器的译码速度和吞吐量。因此本文所提出的算法不仅为多元 LDPC 码的应用提供了一个良好的理论支撑, 也具有一定的工程价值。

参 考 文 献

- [1] Gallager R G. Low-Density Parity-Check codes [J]. *IRE Transactions on Information Theory*, 1962, 8(1): 21–28.
 - [2] Davey M C and MacKay D J C. Low-density parity check codes over $GF(q)$ [J]. *IEEE Communications Letters*, 1998, 2(6): 165–167.
 - [3] Hu X Y and Eleftheriou E. Binary representation of cycle tanner-graph $GF(2^b)$ codes [C]. IEEE International Conference on Communications, Paris, France, 2004: 528–532.
 - [4] Hassani S, Hamon M, and P'enard P. A comparison study of binary and non-binary LDPC codes decoding [C]. The 19th International Conference on Software, Telecommunications and Computer Networks, Dalmatia, Croatia, 2010: 355–359.
 - [5] Lin W, Bai B, Li Y, *et al.* Design of q -ary irregular repeat-accumulate codes [C]. International Conference on Advanced Information Networking and Applications, Bradford, 2009: 201–206.
 - [6] Zeng L, Lan L, Tai Y, *et al.* Constructions of nonbinary quasi-cyclic LDPC codes: a finite field approach [J]. *IEEE Transactions on Communications*, 2008, 56(4): 545–554.
 - [7] Zeng L, Lan L, Tai Y, *et al.* Constructions of nonbinary cyclic, quasi-cyclic and regular LDPC codes: a finite geometry approach [J]. *IEEE Transactions on Communications*, 2008, 56(3): 378–387.
 - [8] MacKay D J C and Davey M C. Evaluation of gallager codes for short block length and high rate application [C]. IMA International Conference on Mathematic and its Applications: Codes, Systems and Graphical Models, New York, 2000: 113–133.
 - [9] Declercq D and Fossorier M. Extended min-sum algorithms for decoding LDPC codes over $GF(q)$ [J]. *IEEE Transactions on Information Theory*, 2007, 55(4): 633–643.
 - [10] Voicila A, Declercq D, Verdier F, *et al.* Low-complexity decoding for non-binary LDPC codes in high order fields [J]. *IEEE Transactions on Communications*, 2010, 58(5): 1355–1375.
 - [11] Sun Y, Zhang Y, Hu J, *et al.* FPGA implementation of nonbinary quasi-cyclic LDPC decoder based on EMS algorithm [C]. International Conference on Communications, Circuits and Systems, Milpitas, California, 2009: 1061–1065.
 - [12] Lin J, Sha J, Wang Z, *et al.* Efficient decoder design for nonbinary quasicyclic LDPC codes [J]. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2010, 57(5): 1071–1082.
 - [13] Poulliat C, Fossorier M, and Declercq D. Design of regular $(2, d_c)$ -LDPC codes over $GF(q)$ using their binary images [J]. *IEEE Transactions on Communications*, 2008, 56(3): 1626–1635.
- 何光华: 男, 1984 年生, 博士生, 研究方向为差错控制编码和数字信号处理。
白宝明: 男, 1966 年生, 博士, 教授, 博士生导师, 研究方向为信道编码、无线通信和量子通信。
王雪鹏: 男, 1987 年生, 硕士生, 研究方向为信息论及信道编码。