

比特交织串行级联 MSK 系统性能分析

张志军¹, 王卫锋², 段新涛¹

(1. 河南师范大学 计算机与信息工程学院, 河南 新乡 453007;

2. 新乡学院 计算机与信息工程学院, 河南 新乡 453000)

摘要:研究了在接收端采用联合迭代解调和译码的比特交织的串行级联 MSK 系统. 与采用简单相移键控载波调制的串行级联码相比, 比特交织串行级联 MSK 系统可以获得更高的带宽效率. 理论分析和性能仿真结果表明: 比特交织器的类型对系统性能的影响非常大, 伪随机比特交织是理想的选择方案, 串行级联 MSK 系统的性能随着交织长度增加而提高; 串行级联 MSK 系统的误比特性能随着迭代次数增加而提高; 当迭代次数达到一定次数之后, 继续增加迭代次数对系统性能的改善有限, 通常迭代次数 < 12 次; 约束长度为 3 的卷积码是外码比较好的选择.

关键词: 迭代译码; MSK; 串行级联编码

中图分类号: TN911.22 **文献标志码:** A **DOI:** 10.3969/j.issn.2095-476X.2013.04.020

Performance analysis of serially concatenated minimum shift keying with bit-interleaver

ZHANG Zhi-jun¹, WANG Wei-feng², DUAN Xin-tao¹

(1. College of Computer and Information Engineering, Henan Normal University, Xinxiang 453007, China;

2. College of Computer and Information Engineering, Xinxiang University, Xinxiang 453000, China)

Abstract: The serially concatenated minimum shift keying (MSK) system with bit-interleaver when the receiver employs iterative decoding and demodulation was investigated. Compared with serially concatenated code which employed traditional shift keying modulation, serially concatenated MSK with bit-interleaver had a better performance with high bandwidth efficiency. Theoretical analysis and performance simulation results showed that: The influence of interleaving scheme system performance was very large and the pseudo-random interleaver was the ideal option; meanwhile, serial concatenated MSK system performance improved with the increase of the interleaving length and the number of iterations. When the number of iterations reached a certain number of times, continuous increase of the number of iterations had limited function in the performance improvement of the system. Usually the number of iterations was less than 12 times. The outer code was convolutional code with constraint length 3, which was a better choice.

Key words: iterative decoding; minimum shift keying (MSK); serial concatenated codes

0 引言

现代无线通信系统要求传输速率高、抗误码能力强,并兼顾带宽和功率有效性. 最小相移键控 MSK(minimum shift keying) 调制技术广泛地应用在无线通信系统中,主要是由于它具有较高频谱利用率和恒包络特点,从而可以使用工作在饱和状态的非线性放大器^[1]. 文献[2]证明了 MSK 调制器可以分解为一个连续相位编码器跟随一个无记忆调制器,也就是 MSK 调制可以看成一种编码调制. 随着编码理论不断发展,在 Turbo 码^[3] 提出后不久,S. Benedetto 等^[4] 证明了串行级联码比 Turbo 码(也被称为并行级联码)具有更陡峭的瀑布区和更低的错误平台. 并且由 MSK 调制作为串行级联码内码构成的串行级联 MSK 系统,其带宽效率远高于采用简单的串行级联码相移键控载波调制^[1,5-7]. 鉴于此,本文拟研究比特交织的串行级联 MSK 系统的性能,分析系统的各个参数对系统性能的影响,以期给出比特交织的串行级联 MSK 系统的参数设计原则.

1 串行级联 MSK 系统模型

图 1 给出了一个在接收端采用联合迭代解调和译码的串行级联 MSK 系统框图. 图中包括卷积码编码器、交织器、MSK 调制器和联合迭代解调译码器. 对于每一帧信号, K 个独立的信息序列送入到卷积码编码器得到输出编码符号序列 $X = (x_1, x_2, \dots, x_N)$, 然后送到比特交织器. 交织后的信息序列 $\tilde{X} = (\tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_N)$ 最后经 MSK 调制送入无线信道中.

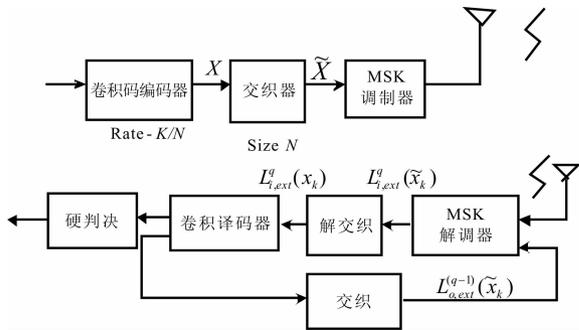


图 1 串行级联 MSK 系统框图

1.1 MSK 调制器

MSK 调制器可以分解为一个码率为 1/2 的连续相位编码器和一个无记忆调制器,但是这种 MSK 的编码调制描述形式不是惟一的^[8-10],连续相位编

码器可分为非递归(图 2)和递归(图 3)2 种形式. 连续相位编码器的输出为 2 元数组 (a, b) , 其中 $a, b \in \{0, 1\}$. 对于非递归形式的连续相位编码器,其输出后的无记忆编码器按照下式进行波形映射:

$$s(t, x) = \begin{cases} A \cos(2\pi f_1 t), & \text{if } a = 0, b = 0 \\ A \cos(2\pi f_2 t), & \text{if } a = 0, b = 1 \\ -A \cos(2\pi f_2 t), & \text{if } a = 1, b = 0 \\ -A \cos(2\pi f_1 t), & \text{if } a = 1, b = 1 \end{cases}$$

递归形式表示的无记忆编码器按下式规则进行波形映射:

$$s(t, x) = \begin{cases} A \cos(2\pi f_1 t), & \text{if } a = 0, b = 0 \\ -A \cos(2\pi f_1 t), & \text{if } a = 0, b = 1 \\ A \cos(2\pi f_2 t), & \text{if } a = 1, b = 0 \\ -A \cos(2\pi f_2 t), & \text{if } a = 1, b = 1 \end{cases}$$

在波形映射规则中, A 是 MSK 调制波信号的振幅值, 2 个载波频率的差值满足等式 $(f_2 - f_1) = 1/(2T)$, T 为 MSK 输入端的每个信息符号的持续间隔.

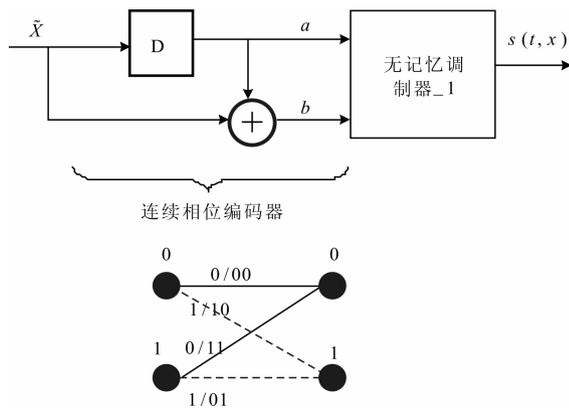


图 2 MSK 调制器的非递归描述方式和对应的格图

1.2 接收端

发送端发射的信号经 AWGN 信道传输后,接收到的受噪声干扰的信号可表示成 $\gamma = (r_1, r_2, \dots, r_N)$, 其中每个分量为 $r_k = (r_{k,1}, r_{k,2}) = s_k + n_k$, n_k 是均值为 0, 双边带功率谱密度为 $N_0/2$ 的加性高斯噪声矢量. 本文主要研究接收端采用联合迭代解调和译码的串行级联 MSK 系统,最大迭代次数用 Q 表示. 联合迭代步骤可描述为:

步骤 1: 第 q 次联合迭代中, MSK 解调器利用信道接收信号 $\gamma = (r_1, r_2, \dots, r_N)$ 和第 $(q-1)$ 次迭代后的外码外信息 $L_{\alpha, ext}^{(q-1)}(\tilde{X})$ 采用 BCJR 算法^[11] 计算序列 $\tilde{X} = (\tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_N)$ 中每个比特的对数似然比

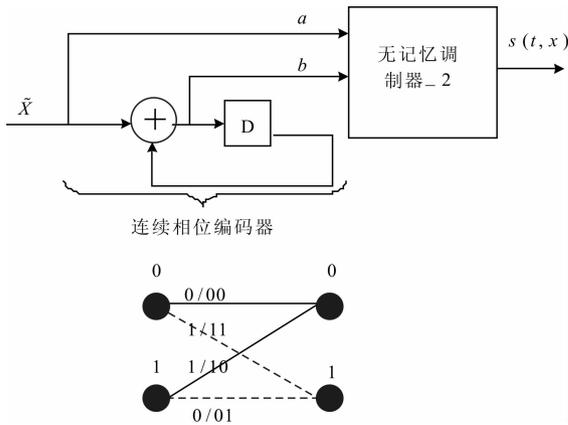


图3 MSK 调制器的递归描述方式和对应的格图

$$L_i^{(q)}(\tilde{x}_k) = \log \frac{P(\tilde{x}_k = 0 | \gamma, L_{0,ext}^{(q-1)}(\tilde{X}))}{P(\tilde{x}_k = 1 | \gamma, L_{0,ext}^{(q-1)}(\tilde{X}))}$$

MSK 解调器输出的内码的外信息为

$$L_{i,ext}^{(q)}(\tilde{x}_k) = L_i^{(q)}(\tilde{x}_k) - L_{i,ext}^{(q-1)}(\tilde{x}_k), \forall k$$

步骤 2: 第 q 次联合迭代时, MSK 解调器输出的内码外信息 $L_{i,ext}^{(q)}(\tilde{x}_k)$ 解交织后 $L_{i,ext}^{(q)}(x_k)$ 送到卷积译码器, 卷积译码器将解交织后的内码外信息 $L_{i,ext}^{(q)}(x_k), \forall k$ 视同“信道接收的信号”利用 BCJR 算法^[11] 计算外码的外信息 $L_{o,ext}^{(q)}(x_k), \forall k$.

步骤 3: 卷积译码器输出的外码外信息 $L_{o,ext}^{(q)}(X)$ 经交织后 $L_{o,ext}^{(q)}(\tilde{X})$ 送到 MSK 解调器以供第 $q+1$ 次迭代使用.

上述联合迭代过程持续进行 Q 次. 当 $Q=0$ 时, 对应的是没有迭代的情形. K. R. Narayanan 等^[10] 已经证明, 在 AWGN 信道中, 如果 MSK 采用非递归分解模式, 系统不需要迭代解调, 因此, 在仿真中 MSK 采用递归分解模式.

2 系统交织器、迭代次数和卷积码对系统的影响

比特交织串行级联 MSK 系统的误比特性能可以由其联合界得出. 基于联合界的误比特率分析假定级联系统采用最大似然序列检测和均匀比特交织器, 而实际中往往采用次优迭代解码器和伪随机比特交织器. 下面采用仿真的方法, 分别从交织器类型、迭代次数和外码的选择 3 个方面来考察串行级联 MSK 系统的各个参数对系统性能的影响. 系统仿真中, 当统计的比特错误数 > 100 , 或者数据帧数 $> 20\ 000$ 帧时, 仿真终止.

2.1 交织器的影响

比特交织器是影响迭代解码器性能的重要因

素, 是决定级联编码系统在误比特小于 10^{-2} 大于 10^{-5} 区域性能的关键因素之一. 从图 4 所示的仿真结果可以看出, 相对于分组比特交织方案, 采用伪随机比特交织方案可以显著地提高系统的性能. 下面分析采用伪随机比特交织下、交织长度为 256, 512, 1 024, 2 048, 3 072, 4 096 时, 对比特交织串行级联 MSK 系统性能的影响, 卷积码的生成多项式为 $(5, 7)_8$. 图 4 中系统参数为卷积码 $(5, 7)_8$, AWGN 信道. 从图 5 所示的仿真结果可以看出, 比特交织串行级联 MSK 系统联合迭代解调译码的误比特性能随着交织长度的增加而降低. 当信噪比较低时, 交织长度的增加对系统误比特性能的改善不是很大. 随着信噪比的增大, 系统误比特性能的改善随着交织的长度的增加先快后慢. 图 5 中系统参数为卷积码 $(5, 7)_8$, 迭代 16 次, AWGN 信道.

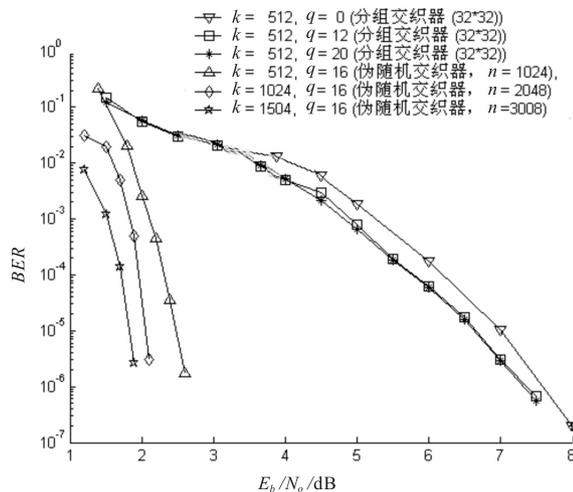


图4 比特交织器类型对系统性能的影响

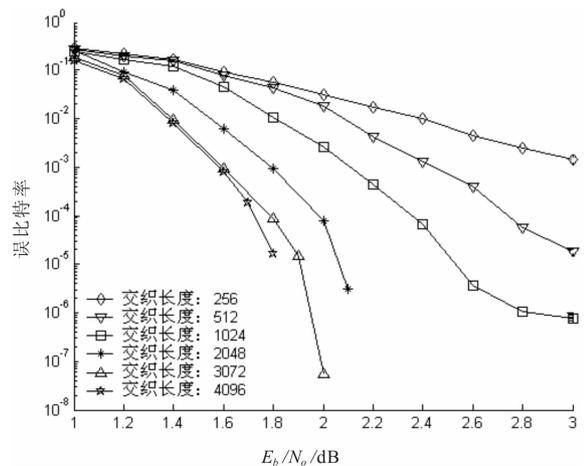


图5 比特交织长度变化对串行级联 MSK 系统性能的影响

2.2 迭代次数的影响

比特交织串行级联 MSK 系统采用联合迭代解调译码的方法来优化系统的误比特性能,因此迭代次数是设计比特交织串行级联 MSK 系统的重要参数.下面分析交织长度为 3 008,卷积码的生成多项式为 $(5,7)_8$ 时,迭代次数对比特交织串行级联 MSK 系统性能的影响.从图 6 的仿真结果可以看出,随着迭代次数的增加,比特交织串行级联 MSK 系统的误比特性能不断地降低并趋于收敛;在瀑布区域,随着信噪比的增大,迭代对系统性能的影响越明显;随着信噪比的进一步增大,可以看到错误平层的存在.图 6 中系统参数为卷积码 $(5,7)_8$,交织长度 3 008,AWGN 信道.

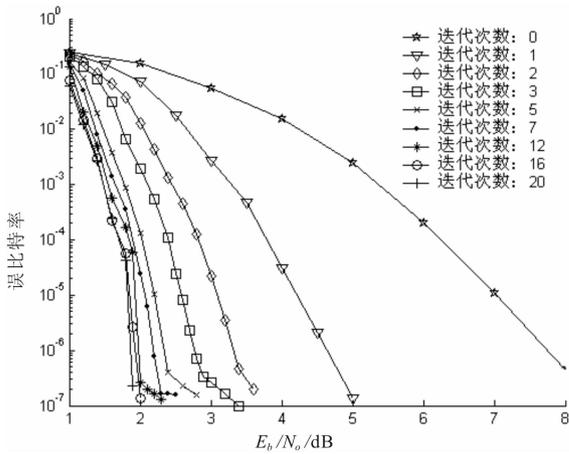


图 6 迭代次数对比特交织串行级联 MSK 系统性能的影响

2.3 卷积码的影响

串行级联编码系统中外码的自由距离影响到交织增益.下面分析交织长度为 3 008,迭代 16 次时,约束长度为 3,4,5,6 的 4 种码率为 1/2 的卷积码对串行级联 MSK 系统性能的影响,卷积码的生成多项式分别是 $(5,7)_8$, $(13,17)_8$, $(27,31)_8$ 和 $(53,75)_8$.图 7 中系统参数为交织长度 3 008,迭代 16 次,AWGN 信道.从图 7 的仿真结果可以看出,随着信噪比的增大,不同约束长度的比特交织串行级联 MSK 系统的误比特性能区别开始增大.信噪比小于约 1.2 dB,所分析的 4 种系统的性能区别不是很明显;信噪比介于 1.2 dB 和 1.6 dB 之间、约束长度为 4,5,6 的 3 个系统的误比特系统,其区别不是很明显,而约束长度为 2 的系统误比特性能要明显地优于其他另外 3 个系统;当误比特为 10^{-5} 时,4 种约束长度的比特交织串行级联 MSK 系统所需要的信噪

比随着约束长度的增加而增大.

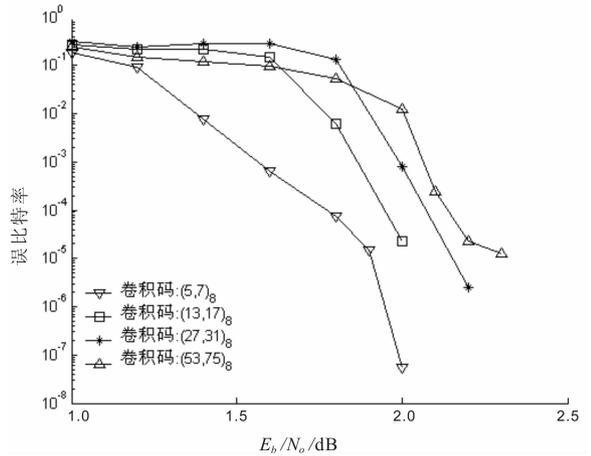


图 7 不同约束长度的外码对串行级联 MSK 系统性能的影响

3 结语

本文对比特交织串行级联 MSK 系统进行了研究,由于系统的码率完全由外码的码率决定,对深空通信、卫星通信等期望获得高谱利用率和较大的编码增益的系统来讲,采用联合迭代解调译码的串行级联 MSK 系统可以提供较好的解决方案.通过上面的仿真结果及分析,可以得出以下结论:

- 1) 比特交织器的类型对系统性能的影响非常大,伪随机比特交织是理想的选择方案;同时串行级联 MSK 系统的性能随着交织长度增加而提高.
- 2) 串行级联 MSK 系统的误比特性能随着迭代次数增加而提高,当迭代次数达到一定次数之后,继续增加迭代次数对系统性能的改善有限,通常迭代次数 < 12 次.
- 3) 约束长度为 3 的卷积码是外码比较好的选择.

参考文献:

[1] 孙锦华,吴小钧,向茜.符号交织 SCCPM 的设计与性能分析[J].西安电子科技大学学报:自然科学版,2012,39(1):23.
 [2] Rimldi B. A decomposition approach to CPM[J]. IEEE Transactions on Information Theory,1988,34(2):260.
 [3] Berrou C,Glavifux A,Thitimajshima P. Near shannon limit error-correcting coding and decoding: turbo-codes [C]//Proc of ICC'93,Piscataway:Institute of Electrical and Electronics Engineers Inc,1993:1064 - 1070.

为 TTGTCTCGAGTTCGAGTGC GCAA, 这一 DNA 序列很有可能是目的基因, 因为三联体的排列完全符合表 1 所示编码方式. 有了编码方式, 攻击者可以验证分离出的 DNA 分子是否为重组 DNA 分子, 因此, 公开编码方式会降低安全性.

3 特点与缺陷

特点是重组 DNA 与冗余 DNA 混合在一起, 受体细菌与冗余细菌混合在一起, 明文得到了两度隐藏; 随机尝试, 可能既破坏明文又得不到密文.

缺陷是细菌抗药性可能发生变异, 冗余细菌的抗药性可能变得和受体细菌相同, 从而使正确的接收方也无法解密; 大量使用抗生素可能导致细菌产生更强的抗药性, 对人类产生危害.

4 结论

利用重组 DNA 技术、结合抗生素杀菌作用以及细菌抗药性提出了以细菌 DNA 为载体的信息隐藏方案. 信息得到了两度隐藏, 不知道密钥, 可能会既毁灭了密文也得不到明文. 今后的研究还需进一步对该方案进行评估与改进.

参考文献:

[1] Chang W L, Guo M, Ho M S H. Fast parallel molecular algorithms for DNA-based computation; factoring integers

[J]//IEEE Transactions on Nanobioscience, 2005, 4(2):149.

- [2] Zhang X C, Niu Y, Cui G, et al. Breaking the NTRU public-key cryptosystem using self-assembly of DNA tilings [J]. Chinese Journal of Computers, 2008, 12(31):2129.
- [3] 杨学庆, 柳重堪. 基于 DNA 计算的 RSA 密码系统攻击方法[J]. 计算机工程, 2010, 36(2):1.
- [4] Celland C, Risca V, Bancroft C. Hiding messages in DNA microdots [J]. Nature, 1999, 399(6736):533.
- [5] 肖国镇, 卢明欣, 秦磊, 等. 密码学的新领域——DNA 密码[J]. 科学通报, 2006, 51(10):1139.
- [6] 卢明欣, 来学嘉, 肖国镇, 等. 基于 DNA 技术的对称加密方法[J]. 中国科学, 2007, 37(2):175.
- [7] 来学嘉, 卢明欣, 秦磊, 等. 基于 DNA 技术的非对称加密与签名方法[J]. 中国科学, 2010, 40(2):240.
- [8] Chen Z H, Xu J. One-Time-Pads encryption in the tile assembly model [J]. Journal of Computational and Theoretical Nanoscience, 2010, 7(5):848.
- [9] Hirabayashi M, Kojima H, Oiwai K. Design of true random one-time pads in DNA XOR cryptosystem [J]. Proceedings in Information and Communications Technology, 2010(2):174.
- [10] 蒋君, 殷志祥. DNA 密码对比传统密码学与量子密码学的优势与不足[J]. 科技视界, 2012, 24:24.
- [11] 饶妮妮. 一种基于重组 DNA 技术的密码方案[J]. 电子学报, 2004, 32(7):1216.

(上接第 85 页)

- [4] Benedetto S, Divsalar D, Montorsi G, et al. Pollara. Serial concatenation of interleaved codes: Performance analysis, design, and iterative decoding [J]. IEEE Transactions on Information Theory, 1998, 44(3):909.
- [5] Ming Xiao, Tor Aulin. Serially concatenated continuous phase modulation with convolutional codes over rings [J]. IEEE Transaction on Communication, 2006, 54(8):1387.
- [6] Maw R L, Taylor D P. Space-time coded systems using continuous phase modulation [J]. IEEE Transaction on Communication, 2007, 55(11):2047.
- [7] Zhang Zhijun, Zhang Aili, Fu Huan. Performance study on convolutional coded MSK system [C]//The 7th International Conference on Wireless Communication, Networking and Mobile Computing, Piscataway: Institute of Electrical

and Electronics Engineers Inc, 2011:1074-1076.

- [8] Zhang Zhijun, Yang Yujie, Wang Xianfang, et al. Serially concatenated coded M-ary continuous phase modulation with bit-interleaver [J]. Journal of Theoretical and Applied Information Technology, 2012, 45(1):144.
- [9] Zhang Zhijun, Wang Weifeng, Xintao Duan. Performance analysis of Q-ary low-density parity-check coded continuous phase modulations [J]. International Review on Computers and Software, 2012, 7(7):3665.
- [10] Narayanan K R, Altunbas I, Narayanswami R S. Design of serial concatenated MSK schemes based on density evolution [J]. IEEE Transaction on Communication, 2003, 51(8):1283.
- [11] Bahl L, Cocke J, Jelinek F, et al. Optimal decoding of linear codes for minimizing symbol error rate [J]. IEEE Transactions on Information Theory, 1974, 20(2):284.