



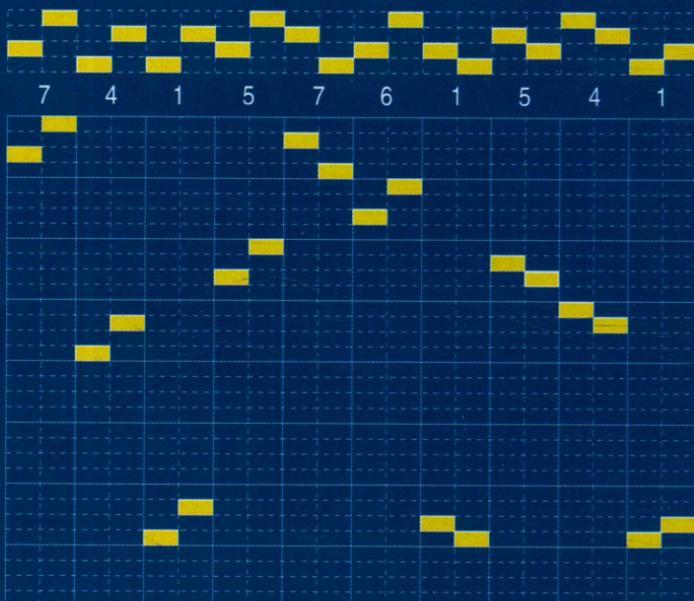
国防科技图书出版基金

跳频序列设计

Frequency Hopping Sequences Design

梅文华 著

0111001000100111100001110100100111100001



国防工业出版社

National Defense Industry Press



国防科技图书出版基金

跳频序列设计

Frequency Hopping Sequences Design



国防工业出版社

·北京·

图书在版编目(CIP)数据

跳频序列设计 / 梅文华著 . —北京 : 国防工业出版社, 2016. 1

ISBN 978 - 7 - 118 - 10386 - 1

I . ①跳… II . ①梅… III . ①跳频—通信系统—
序列—设计 IV . ①TN914. 41

中国版本图书馆 CIP 数据核字(2015)第 279116 号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号 邮政编码 100048)

国防工业出版社印刷厂印刷

新华书店经售

*

开本 880×1230 1/32 印张 10 1/8 字数 305 千字

2016 年 1 月第 1 版第 1 次印刷 印数 1—2000 册 定价 55.00 元

(本书如有印装错误, 我社负责调换)

国防书店: (010) 88540777

发行邮购: (010) 88540776

发行传真: (010) 88540755

发行业务: (010) 88540717

致 读 者

本书由国防科技图书出版基金资助出版。

国防科技图书出版工作是国防科技事业的一个重要方面。优秀的国防科技图书既是国防科技成果的一部分,又是国防科技水平的重要标志。为了促进国防科技和武器装备建设事业的发展,加强社会主义物质文明和精神文明建设,培养优秀科技人才,确保国防科技优秀图书的出版,原国防科工委于1988年初决定每年拨出专款,设立国防科技图书出版基金,成立评审委员会,扶持、审定出版国防科技优秀图书。

国防科技图书出版基金资助的对象是:

1. 在国防科学技术领域中,学术水平高,内容有创见,在学科上居领先地位的基础科学理论图书;在工程技术理论方面有突破的应用科学专著。
2. 学术思想新颖,内容具体、实用,对国防科技和武器装备发展具有较大推动作用的专著;密切结合国防现代化和武器装备现代化需要的高新技术内容的专著。
3. 有重要发展前景和有重大开拓使用价值,密切结合国防现代化和武器装备现代化需要的新工艺、新材料内容的专著。
4. 填补目前我国科技领域空白并具有军事应用前景的薄弱学科和边缘学科的科技图书。

国防科技图书出版基金评审委员会在总装备部的领导下开展工作,负责掌握出版基金的使用方向,评审受理的图书选题,决定资助的图书选题和资助金额,以及决定中断或取消资助等。经评审给予资助的图书,由总装备部国防工业出版社列选出版。

国防科技事业已经取得了举世瞩目的成就。国防科技图书承担着记载和弘扬这些成就,积累和传播科技知识的使命。在改革开放的新形势下,原国防科工委率先设立出版基金,扶持出版科技图书,这是一项具有深远意义的创举。此举势必促使国防科技图书的出版随着国防科技事业的发展更加兴旺。

设立出版基金是一件新生事物，是对出版工作的一项改革。因而，评审工作需要不断地摸索、认真地总结和及时地改进，这样，才能使有限的基金发挥出巨大的效能。评审工作更需要国防科技和武器装备建设战线广大科技工作者、专家、教授、以及社会各界朋友的热情支持。

让我们携起手来，为祖国昌盛、科技腾飞、出版繁荣而共同奋斗！

国防科技图书出版基金

评审委员会

国防科技图书出版基金 第六届评审委员会组成人员

主任委员 王 峰

副主任委员 宋家树 蔡 镛 杨崇新

秘 书 长 杨崇新

副 秘 书 长 邢海鹰 贺 明

委 员 于景元 才鸿年 马伟明 王小摸 甘茂治
(按姓氏笔画排序) 甘晓华 卢秉恒 邬江兴 刘世参 芮筱亭

李言荣 李德仁 李德毅 杨 伟 肖志力

吴有生 吴宏鑫 何新贵 张信威 陈良惠

陈冀胜 周一宇 赵万生 赵凤起 崔尔杰

韩祖南 傅惠民 魏炳波

前　　言

随着通信领域的电波斗争愈演愈烈,惯用的定频通信受到了严重威胁。为了保证己方正常可靠地通信,一种抗干扰通信体制——跳频通信系统应运而生。可以说,在现代战争中,如果无线通信装备不采用抗干扰措施,就没有生存能力。

西方国家早在 20 世纪 50 年代就开始进行一系列的抗干扰通信体制和抗干扰技术的理论研究。到 20 世纪 80 年代初,大部分抗干扰技术都已陆续应用于新的通信装备和系统中,而且还在不断改进和完善。1982 年,英国在马尔维纳斯群岛(福克兰群岛)战争中使用了跳频电台。1991 年的海湾战争中,多国部队为提高通信的抗截获、抗干扰能力,普遍使用了跳频通信装备,如美国的 Sincgars 系列超短波跳频电台和联合战术信息分发系统 JTIDS、英国的 Jaguar-V 和法国的 TRC-950 等超短波跳频电台。

跳频通信技术具有优良的抗干扰性能和多址组网性能,不但在军事通信中得到了广泛应用,而且与我们的日常生活密切相关,在民用移动通信中也得到了广泛的应用,如 GSM、蓝牙中都应用了跳频技术。

实现跳频通信,需要在常规定频通信技术的基础上,解决跳频序列设计、跳频频率合成、跳频同步和组网等几个关键技术。跳频序列的性能对跳频通信系统的性能有着决定性的影响,如果跳频序列设计得不好,即使跳频通信系统的硬件电路设计得非常出色,也达不到抗干扰的目的。寻求和设计具有理想性能的跳频序列是研究跳频通信系统的重要课题之一。本书正是要探讨跳频序列设计的有关知识。

全书共分为 16 章。第 1 章概述,阐述研究的背景和有关概念;第 2 章跳频序列设计的理论限制,阐述跳频序列设计时频率数目、序列周期、序列数量、汉明相关、跳频间隔等几个参数之间的约束关系;第 3 章

至第 14 章分别阐述素数跳频序列族及其变型、基于 m 序列构造跳频序列族、基于 RS 码构造跳频序列族、基于 M 序列构造跳频序列族、基于 GMW 序列构造跳频序列族、基于 $GF(p^m)$ 上的伪随机序列构造最佳跳频序列族、基于 Bent 函数构造跳频序列族、混沌跳频序列族、非重复跳频序列族、宽间隔跳频序列族、蓝牙跳频序列族、基于密码学的跳频序列设计；第 15 章阐述其他跳频序列族设计，包括基于同余式构造跳频序列族、基于组合设计的跳频序列设计、基于云模型的跳频序列设计、差分跳频的 G 函数算法、NHz/LHz 跳频序列设计、雷达跳频编码设计；第 16 章阐述跳频序列设计需要考虑的因素。在附录中提供了 $GF(2)$ 上的 n 级本原多项式 ($2 \leq n \leq 100$)、 $GF(p)$ 上的 n 级本原多项式 ($2 \leq p \leq 127, p^n < 2^{32}$)、 $GF(2^m)$ 上的 n 级本原多项式 ($mn \leq 32$)、素数及其最小原根表 (5000 以内)。

作者衷心感谢周炯槃院士、王越院士、王小谟院士、陆建勋院士、李德毅院士、杨义先教授、周兆祺教授、李承恕教授、陈先福教授的悉心指导；衷心感谢空军装备研究院及航空所、通信所领导和专家的支持帮助。在编写过程中，还得到了周亮教授、王淑波博士、李昊硕士的帮助，在此一并表示感谢。

本书的编著得到了电子科技大学通信抗干扰技术国防科技重点实验室资助，本书的出版得到了国防科技图书出版基金资助，在此一并表示感谢。

谨以此书献给我的父母、岳父母和妻子。正是他们的全力支持，特别是妻子吴文婷 20 多年来的默默付出，使得我可以利用晚上和节假日休息时间开展研究，撰写论著。

作者期望本书的出版能够抛砖引玉，为相关专业的科研人员、工程技术人员以及博士生、硕士生提供参考。由于作者水平有限，缺点和不足在所难免，欢迎批评指正。

梅文华

2015 年 1 月 29 日

目 录

第 1 章 概述	1
1. 1 跳频通信的基本概念	1
1. 2 跳频序列的定义	5
1. 3 跳频序列的汉明相关	6
1. 4 跳频组网方式	11
1. 4. 1 跳频组网分类	11
1. 4. 2 同步正交组网	13
1. 4. 3 同步非正交组网	14
1. 4. 4 异步非正交组网	16
1. 5 跳频序列设计与 TOD	17
1. 6 跳频序列设计的一般要求	18
第 2 章 跳频序列设计的理论限制	20
2. 1 给定频率数目和序列周期条件下汉明相关的理论限	20
2. 2 限定汉明相关条件下序列数量和序列周期的理论限	27
2. 3 非重复跳频序列族的理论限	30
2. 4 非重复宽间隔跳频序列族的理论限	34
2. 5 限定平均汉明相关条件下网络数量的理论限	36
2. 6 跳频序列集周期汉明相关的理论限	37
2. 7 低碰撞区跳频序列集周期汉明相关的理论限	44
第 3 章 素数跳频序列族及其变型	52
3. 1 素数跳频序列族的构造	52
3. 2 素数跳频序列族的性能	54
3. 3 素数跳频序列族达到的理论限	56
3. 4 截短型素数跳频序列族	57

3.5 截短型倒素数跳频序列族	59
3.6 倒素数跳频序列族	65
第4章 基于m序列构造跳频序列族	67
4.1 m 序列的基本原理	67
4.2 m 状态序列 $SM(2^n)$ 作为跳频序列	75
4.3 Lempel-Greenberger 模型	78
4.4 非连续抽头模型	81
4.5 构造最佳跳频序列族的一般模型	86
4.6 基于 $GF(p^r)$ 上 m 序列的构造模型	91
4.6.1 $GF(p^r)$ 上的 m 序列及其性能	91
4.6.2 基于 $GF(p^r)$ 上 m 序列的构造方法	92
4.7 非线性化方法	95
第5章 基于RS码构造跳频序列族	97
5.1 纠错编码的基本原理	97
5.2 RS码的基本原理	99
5.3 RS码的挑选	101
5.4 RS码作为跳频序列的性能	102
5.5 有限域算术运算的实现	105
5.6 RS跳频序列的硬件实现	108
第6章 基于M序列构造跳频序列族	109
6.1 M 序列的构造方法	109
6.2 M 状态序列作为跳频序列	116
6.3 基于 M 序列的抽头选取法	117
6.4 非线性跳频序列族的构造	118
第7章 基于GMW序列构造跳频序列族	122
7.1 GMW序列的构造	122
7.1.1 GMW序列的定义	122
7.1.2 GMW序列的性能	123
7.1.3 GMW序列构造实例	128
7.2 基于GMW序列构造最佳跳频序列族	136
7.3 基于GMW序列构造最佳跳频序列族的广义模型	138

7.4	基于级联 GMW 序列构造最佳跳频序列族	139
第 8 章	基于 $GF(p^m)$ 上的伪随机序列构造最佳跳频序 列族	
8.1	预备知识	141
8.1.1	迹函数及其性质	141
8.1.2	有限域中元素的表示	142
8.1.3	有限域的加法特征	143
8.2	$GF(p^m)$ 上伪随机序列的自相关函数	144
8.2.1	$GF(p^m)$ 上伪随机序列周期自相关函数的定义	144
8.2.2	$GF(p^m)$ 上序列具有二值自相关函数的等价条件	147
8.3	$GF(p^m)$ 上最佳跳频序列族的构造	149
8.3.1	构造方法	149
8.3.2	性能分析	150
第 9 章	基于 Bent 函数构造跳频序列族	153
9.1	q 元 Bent 函数	153
9.2	基于 q 元 Bent 函数构造跳频序列族	164
9.3	Bent 跳频序列族的线性复杂度分析	172
第 10 章	混沌跳频序列族	177
10.1	混沌映射	177
10.1.1	Logistic 映射	177
10.1.2	Tent 映射	179
10.1.3	Chebyshev 映射	180
10.2	实值量化	180
10.2.1	均匀多值量化	180
10.2.2	非均匀多值量化	181
10.3	基于 Logistic 映射构造跳频序列	181
10.3.1	构造方法概述	181
10.3.2	简单非均匀多值量化方法	184
10.3.3	多次迭代非均匀多值量化方法	185
第 11 章	非重复跳频序列族	188
11.1	非重复跳频序列的数量	188

11.2	一次重合的非重复跳频序列族	189
11.3	k 次重合的非重复跳频序列族	200
第 12 章	宽间隔跳频序列族	208
12.1	宽间隔跳频的意义	208
12.2	宽间隔处理方法	209
12.2.1	去中间频带法	209
12.2.2	对偶频带法	213
12.2.3	平移替代法	216
12.2.4	生成序列圆法	218
12.2.5	素数序列构造法	223
12.3	基于素数跳频序列构造宽间隔跳频序列族	225
12.4	基于 m 序列构造宽间隔跳频序列族	233
第 13 章	蓝牙跳频序列族	239
13.1	蓝牙跳频技术	239
13.2	蓝牙跳频序列选频原理	240
13.2.1	蓝牙跳频序列选频总体方案	240
13.2.2	蓝牙跳频序列选频内核	242
13.2.3	选频内核控制字	244
13.3	蓝牙自适应跳频序列构造	245
13.3.1	概述	245
13.3.2	蓝牙自适应跳频过程	246
13.3.3	蓝牙信道分类	248
13.3.4	蓝牙自适应跳频序列选频原理	248
13.3.5	蓝牙自适应跳频状态的控制	250
13.4	蓝牙自适应跳频序列的性能分析	253
13.4.1	蓝牙自适应跳频序列的均匀性	253
13.4.2	蓝牙自适应跳频序列的跳频间隔分布特性	255
13.4.3	蓝牙自适应跳频序列的互相关特性	256
13.4.4	蓝牙自适应跳频序列的自相关特性	257
第 14 章	基于密码学的跳频序列设计	260
14.1	密码学简介	260

14. 2	基于序列密码的跳频序列设计	262
14. 2. 1	序列密码概述	262
14. 2. 2	基于序列密码的跳频序列设计	263
14. 3	基于分组密码的跳频序列设计	263
14. 3. 1	分组密码概述	263
14. 3. 2	数据加密算法标准(DES)	265
14. 3. 3	基于分组密码的跳频序列设计	273
第 15 章	其他跳频序列族设计	279
15. 1	基于同余式构造跳频序列族	279
15. 2	基于组合设计的跳频序列设计	284
15. 3	基于云模型的跳频序列设计	286
15. 4	差分跳频的 G 函数算法	287
15. 5	NHZ/LHZ 跳频序列设计	290
15. 6	雷达跳频编码设计	291
第 16 章	跳频序列设计需要考虑的因素	294
16. 1	跳频序列性能	294
16. 2	与现役跳频电台的互联互通问题	295
16. 3	作战、训练与检测状态问题	296
16. 4	标准化设计问题	296
附录	298
附录 1	GF(2) 上的 n 级本原多项式($2 \leq n \leq 100$)	298
附录 2	GF(p) 上的 n 级本原多项式($2 \leq p \leq 127, p^n < 2^{32}$)	303
附录 3	GF(2^m) 上的 n 级本原多项式($mn \leq 32$)	305
附录 4	素数及其最小原根表(5000 以内)	307
参考文献	311

Contents

Chapter 1	Introduction	1
1. 1	Basic Conception of Frequency Hopping Communication	1
1. 2	Definition of Frequency Hopping Sequences	5
1. 3	Hamming Correlation of Frequency Hopping Sequences	6
1. 4	Frequency Hopping Networking	11
1. 4. 1	Classification for Frequency Hopping Networks	11
1. 4. 2	Synchronous Orthogonal Networking	13
1. 4. 3	Synchronous Non-Orthogonal Networking	14
1. 4. 4	Asynchronous Non-Orthogonal Networking	16
1. 5	Frequency Hopping Sequences Design and TOD	17
1. 6	General Requirements for Frequency Hopping Sequences Design	18
Chapter 2	Theoretical Bounds to Frequency Hopping Sequences Design	20
2. 1	Lower Bounds to the Hamming Correlation with Given Number of Frequency Slots and Length of FH Sequences	20
2. 2	Bounds to the Number of FH Sequences and the Length of FH Sequences with Given Hamming Correlation	27
2. 3	Bounds to the Family of Non-repeating FH Sequences	30
2. 4	Bounds to the Family of Non-repeating FH Sequences with Given Minimum Gap	34
2. 5	Bound to the Number of Networks with Given Average Hamming Correlation	36
2. 6	Bounds to the Periodic Hamming Correlation of the	

Family of FH Sequences	37
2.7 Bounds to the Periodic Hamming Correlation of the Family of FH Sequences with Low Hit Zone	44
Chapter 3 Families of Prime Sequences and its Variations	52
3.1 Construction of Prime Sequences	52
3.2 Properties of Prime Sequences	54
3.3 Bounds which Prime Sequences Have Derived	56
3.4 Truncated Prime Sequences	57
3.5 Hyperbolic Prime Sequences	59
3.6 Extended Hyperbolic Prime Sequences	65
Chapter 4 Families of FH Sequences Based on m-Sequences	67
4.1 Basic Principle of m -Sequence	67
4.2 FH Sequences Based on State m -Sequences	75
4.3 Lempel-Greenberger Model	78
4.4 Nonconsecutive Tapping Model	81
4.5 General Model for Optimal Families of FH Sequences Based on m -Sequences	86
4.6 Optimal Families of FH Sequences Based on m - Sequence over $GF(p^r)$	91
4.6.1 Construction and Properties of m -Sequence over $GF(p^r)$	91
4.6.2 Construction of Optimal Families of FH Sequences Based on m -Sequences over $GF(p^r)$	92
4.7 Nonlinearization Method	95
Chapter 5 Families of FH Sequences Based on Reed- Solomon Codes	97
5.1 Basic Principle of Error Correction Codes	97
5.2 Basic Principle of Reed-Solomon Codes	99
5.3 Selection of Reed-Solomon Codes	101
5.4 Properties of FH Sequences Based on Reed-Solomon Codes	102

5. 5	Implementation of Algorithm in Galois Fields	105
5. 6	Hardware Implementation of FH Sequences Based on Reed-Solomon Codes	108
Chapter 6	Families of FH Sequences Based on M-Sequences	109
6. 1	Construction Methods of M -Sequences	109
6. 2	FH Sequences Based on State M -Sequences	116
6. 3	Tapping Model Based on M -Sequences	117
6. 4	Construction Method of Nonlinear FH Sequences	118
Chapter 7	Families of FH Sequences Based on GMW Sequences	122
7. 1	Construction of GMW Sequences	122
7. 1. 1	Definition of GMW Sequences	122
7. 1. 2	Properties of GMW Sequences	123
7. 1. 3	Construction Examples of GMW Sequences	128
7. 2	Optimal Families of FH Sequences Based on GMW Sequences	136
7. 3	General Model of Optimal Families of FH Sequences Based on GMW Sequences	138
7. 4	Optimal Families of FH Sequences Based on Cascaded GMW Sequences	139
Chapter 8	Families of FH Sequences Based on Pseudo-random Sequence over $GF(p^m)$	141
8. 1	Preliminary Knowledge	141
8. 1. 1	Trace Function and its Properties	141
8. 1. 2	Representation of Elements in Galois Fields	142
8. 1. 3	Add Characteristics in Galois Fields	143
8. 2	Autocorrelation Function of Pseudorandom Sequence over $GF(p^m)$	144
8. 2. 1	Definition of Periodic Autocorrelation Function ...	144
8. 2. 2	Equivalent Condition that Pseudorandom Sequences over $GF(p^m)$ Have Two-level	

Autocorrelation Function	147
8.3 Optimal Families of FH Sequences Based on Pseudo-random Sequence over $GF(p^m)$	149
8.3.1 Construction Model	149
8.3.2 Properties Analysis	150
Chapter 9 Families of FH Sequences Based on Bent Sequences	153
9.1 Bent Sequences over $GF(q)$	153
9.2 Families of FH Sequences Based on Bent Sequences over $GF(q)$	164
9.3 Linear Span of Families of FH Sequences Based on Bent Sequences	172
Chapter 10 Families of FH Sequences Based on Chaotic Sequences	177
10.1 Chaotic Mapping	177
10.1.1 Logistic Mapping	177
10.1.2 Tent Mapping	179
10.1.3 Chebyshev Mapping	180
10.2 Real Value Quantitation	180
10.2.1 Multiple Value Uniform Quantitation	180
10.2.2 Multiple Value Non-uniform Quantitation	181
10.3 Families of FH Sequences Based on Logistic Mapping	181
10.3.1 Introduction to Construction Method	181
10.3.2 A Simple Method with Multiple Value Non-uniform Quantitation	184
10.3.3 An Iterative Method with Multiple Value Non-uniform Quantitation	185
Chapter 11 Families of Nonrepeating FH Sequences	188
11.1 The Number of Nonrepeating FH Sequences	188
11.2 Families of Nonrepeating FH Sequences with One Coincidence	189