文章编号:1000－2367(2016)06－0170－05 DOI:10.16366/j.cnki.1000－2367.2016.06.030

一类基于相对差集的异步跳频序列系统

潘红艳[1],付绍静[2],杜 蛟[3]

(1.长沙商贸旅游职业技术学院 基础课部,长沙 410004;2.国防科学技术大学 计算机学院,长沙 410073;
3.河南师范大学 数学与信息科学学院,河南 新乡 453007)

摘 要:在认知无线电网络中,次级用户要实现相互通信,首先要在共有的一个信道上完成异步的无线电盲交汇.该问题可以通过完备的非同步跳频序列系统,设计相应的算法或者协议来解决.利用设计理论中经典的相对差集,对于任意素数幂 q,构造出了一类新的完备的非同步跳频序列系统.该系统使用 $q-1$ 个信道,含有约 $\lfloor (q+1)/2 \rfloor +2$ 条周期为 $2(q^2-1)$ 的序列.该系统的序列周期长度已经非常接近最优的非同步跳频序列系统,而同时它又含有更多的序列,因此,对设计新的交汇协议来讲更为实用.

关键词:跳频序列系统;序列周期;相对差集

中图分类号:TP309.7 **文献标志码**:A

在认知无线电网络中,任意两个次级用户(secondary users)在相互通信之前,需要首先在它们共有的一个信道上完成交汇(Rendezvous).然而,这样的无线电交汇并不容易成功实现,主要原因如下:(1)授权用户(primary users)对于信道的占有和接入是无法预测的,而次级用户在授权用户需要时,必须为其腾出相应的信道.(2)绝大多数的分布式无线电网络中,并不存在中心控制设备来指导次级用户之间的交汇.(3)认知无线电网络中的不同用户之间的时钟是不同步的,即:它们之间的交汇是异步交汇.(4)一般不能预设一个或几个公共的控制信道来作为无线电用户之间的交汇和信息广播通道,因为这会引起"单点瘫痪"问题.

为解决这一问题,研究者们提出了若干种不同的解决方案.在文献[1－2]中提出了一类基于跳频序列的算法.其具体的数学模型如下:

用 0 到 $N-1$ 这 N 个整数来表示无线电网络中的 N 个可用的信道.假设对于每一个系统里的次级用户,它们的时间都可以被相应的分为等长的时间间隔.设 T 是一个正整数,定义一个周期为 T 的跳频序列为 $u=(u_0,u_1,\cdots,u_{T-1})$,其中 u_i 属于 $\{0,1,\cdots,N-1\}$.另外,$L(u)$ 定义为 $L(u)=(u_1,u_2,\cdots,u_{T-1},u_0)$,即:对序列 u 循环左移一位.对于两个给定的跳频序列 u 和 v,如果 $u_i=v_i=h$,那么就称 u 和 v 在第 i 个时间间隔上在 h 信道上实现了交汇.

在实际的通信过程中,不同的次级用户之间的时钟一般是不能同步的,而且通信的双方又通常不知道对方的可用信道.因此,这就要求不同的次级用户之间能够实现非同步盲交汇.反映在前文提出的跳频序列上,需要构造如下的跳频序列集合:

定义 1 设 H 是若干个定义在信道集 S 上的周期为 T 的跳频序列组成的集合.如果对于任意的 $u,v\in H$ 以及任意的 $k\in\{0,1,\cdots,T-1\}$,都有 $\{u_i:u_i=L^k(v)_i\}=S$,那么 H 就被称为一个完备的非同步跳频序列系统(complete asynchronous channel hopping system),简称为 CACH 系统.称 T 为该系统的周期,称 S 的大小为该系统的信道个数.

收稿日期:2016-09-20;**修回日期**:2016-10-30.

基金项目:国家自然科学基金(61572026)

第 1 作者简介:潘红艳(1975－),女,湖南岳阳人,长沙商贸旅游职业技术学院讲师,研究方向为数学基础理论与应用.

通信作者:付绍静(1984－),男,国防科技大学副教授,博士,硕士生导师,研究方向为密码学、网络安全、信息安全,E-mail:shaojing1984@163.com.

例 1　设 $T=N^2, S=\{0,1,\cdots,N-1\}$ 并且

$$u=(\underbrace{0,0,\cdots,0}_{N},\underbrace{1,1,\cdots,1}_{N},\cdots,\underbrace{N-1,\cdots,N-1}_{N}),$$

$$v=(0,1,\cdots,N-1,0,1,\cdots,N-1,\cdots,0,1,\cdots,N-1).$$

可以直接按照定义验证，$H=\{u,v\}$ 是一个 CACH 系统.

假设有两个次级用户使用同一个 CACH 系统中的两个不同的跳频序列来进行交汇. 如果他们拥有至少一个共同的信道，那么在周期 T 内他们一定会在这个共同的信道上成功交汇；如果他们没有共同的可用信道，那么在周期 T 内他们就无法成功交汇，这样他们双方也就都知道没有共有的可用信道，进而停止交汇的尝试. 因此，一个 CACH 系统可以完全解决至少两个次级用户的非同步盲交汇问题. 通过前面的分析可知，系统的周期 T 决定了最大交汇时间的长度，所以周期 T 越短，所导出的交汇算法就越快.

通过简单的组合计数可以证明，如果一个 CACH 系统的周期为 T，而信道个数为 N，那么就有 $T\geq N^2$. 特别地，当等式成立的时，该系统中最多有 $N+1$ 条序列. 具体证明请参见文献[1－2]. 当 $T=N^2$ 时，称 H 为一个完美(perfect)CACH 系统. 可以直接验证，例 1 中的 $H=\{u,v\}$ 是一个完美 CACH 系统.

到目前为止，还没有学者提出含有超过两个序列的完美 CACH 系统. 事实上，陈小天等人最近在文献[3]中证明，当 N 为素数时，完美 CACH 系统只能含有两个序列，而很多数值实验的证据显示，很可能所有的完美 CACH 系统都只能含有两个序列. 然而，在实际应用中，次级用户的数量往往远多于两个，这样一来，就必须在次级用户之间构建复杂的协议来保证，当任意两个不同的次级用户之间需要通信时，使用的是两个不同的序列. 从这个角度讲，完美 CACH 系统并不十分实用.

本文将考虑 CACH 系统的构造问题. 具体来讲，将考虑信道总数为 N 而周期为 αN^2 的 CACH 系统 H 的构造. 这里 α 是一个大于 1 但是尽量接近 1 的实数. 同时，又要求构造出的 CACH 系统 H 中有足够多的序列. 事实上，通过松弛差集(relaxed difference set)，在文献[3－5]中都构造出了周期较短的 CACH 系统. 例如，文献[5]中构造出的 CACH 系统所对应的周期大约为 $3N^2$，这里要求 N 为一个素数. 本文的主要结果为一个信道总数为 N，周期大约为 $2N^2$ 的 CACH 系统，该系统中含有大约 $N/2$ 条序列.

1　预备知识

本节首先介绍差集和相对差集等组合设计的基本概念. 关于它们的性质、构造及其他相关结果，感兴趣的读者可以参考文献[6].

定义 2　设 G 为一个 v 阶群，D 为一个 G 的 k 子集. 如果对于 G 中的每一个非单位元 a，都存在 λ 对 D 中的元素 (d_i,d_j)，使得 $a=d_id_j^{-1}$，那么 D 就被成为一个 (v,k,λ)- 差集(difference set).

定义 3　设 G 为一个 mn 阶群，M 是它的一个 m 阶子群，而 D 为一个 G 的 k 子集. 如果对于 $G\backslash M$ 中的每一个元素 a，都存在 λ 对 D 中的两个不同元素 (d_i,d_j)，使得 $a=d_id_j^{-1}$；并且 M 中的任意元素都不能表示为 $d_id_j^{-1}$ 的形式，其中 $d_i,d_j\in D$，那么就称 D 为一个 (n,m,k,λ)- 相对差集(relative difference set)，而 M 是其相对应的禁子群.

通过比较定义 2 和定义 3 不难发现，当一个相对差集的禁子群为单位元群时，这个相对差集就是一个差集. 因此相对差集可以看作是差集的一个推广，而差集可以视为相对差集的特殊情况. 下面给出一个经典的基于有限射影平面的相对差集.

引理 1[7－8]　设 q 为一个素数幂，G 为有限域 F_{q^n} 的乘法群. 设 $\mathrm{Tr}_{q^n/q}:F_{q^n}\to F_q$ 为 F_{q^n} 到 F_q 的迹函数，即：$\mathrm{Tr}_{q^n/q}(x)=\sum_{i=0}^{n-1}x^{q^i}, x\in F_{q^n}$. 定义

$$D=\{x\in F_{q^n}:\mathrm{Tr}_{q^n/q}(x)=1\}.$$

那么集合 D 是一个 $((q^n-1)/q-1,q-1,q^{n-1},q^{n-2})$- 相对差集，而其禁子群 M 为 F_q 的乘法群. 特别地，当 $n=2$ 时，D 是一个 $(q+1,q-1,q,1)$- 相对差集.

2　一类基于相对差集的构造

本节利用引理 1 来构造一组跳频序列. 首先构造一条具有较好交汇性能的跳频序列 u.

定理 1 设 $n=2$,而 G,q,M 和 D 如引理 1 中所定义,e 为群 G 中的单位元. 令 $E=\{x\in F_{q^2}^*:\mathrm{Tr}_{q^2/q}(x)=0\}$,$\varphi$ 是从 G 到 q^2-1 阶循环群 Z_{q^2-1} 的同构映射. 对于任意的 $a\in G$,定义 $aD=\{ax:x\in D\}$. 如果令

$$\Omega=\{aD:a\in M\}\cup\{E\},$$

那么 Ω 中的所有子集构成 G 的一个剖分. 进一步,按照如下的规则定义周期为 q^2-1 的跳频序列 u:

$$u_i=\begin{cases}e, & i\in\varphi(E);\\ a, & i\in\varphi(aD).\end{cases}$$

其中 $a\in M$(这意味着序列 u 所使用的信道在这里通过 M 中的元素来表示,共 $q-1$ 个),那么序列 u 满足

$$\{u_i:u_i=L^l(u)_i,i=0,1,\cdots,q^2-2\}=\begin{cases}M, & l\notin\varphi(M);\\ \{e\}, & l\in\varphi(M).\end{cases}\tag{1}$$

证明 首先证明 Ω 构成群 G 的一个剖分. 由于 $D=\{x\in F_{q^2}:\mathrm{Tr}_{q^2/q}(x)=x+x^q=1\}$,所以当 $a\in M$ 时,

$$aD=\{ax\in F_{q^2}:\mathrm{Tr}_{q^2/q}(x)=1\}=\{y\in F_{q^2}:\mathrm{Tr}_{q^2/q}(y)=a\}.$$

进一步,由于迹函数是一个满射,所以

$$G=\bigcup_{a\in F_q}\{y\in F_{q^2}:\mathrm{Tr}_{q^2/q}(y)=a\}=\Big(\bigcup_{a\in F_q,a\neq0}aD\Big)\cup E.$$

即:Ω 构成群 G 的一个剖分.

下面来进一步证明序列 u 满足(1)式. 首先考虑 u 中 $i\in\varphi(aD)$ 的位置. 根据 u 的定义,若 $a\neq e$,则 $\{i:u_i=a\}=\varphi(aD)$;若 $a=e$,则 $\{i:u_i=e\}\supset\varphi(D)$. 由于所有的 aD 同 D 一样,也是一个 $(q+1,q-1,q,1)$-相对差集(平移一个相对差集仍得到一个相同参数的相对差集),所以对于任意的 $l\in\varphi(G\backslash M)$,总存在一对 $x,y\in aD$,使得 $l=\varphi(xy^{-1})=\varphi(x)-\varphi(y)$. 如果令 $j=\varphi(x),i=\varphi(y)$,那么就有 $u_i=u_j=a,j-i=l$,即:$u_i=L^l(u)_i=a$. 因此,当 $l\notin\varphi(M)$ 时,就有

$$\{u_i:u_i=L^l(u)_i,i=0,1,\cdots,q^2-2\}=M.$$

另一方面,当 $l\in\varphi(M)$ 且 $l\neq0$ 时,那么作为一个 $(q+1,q-1,q,1)$- 相对差集,aD 中不存在 x,y,使得 $l=\varphi(xy^{-1})=\varphi(x)-\varphi(y)$. 如果设 $a\neq e$,并且令 $j=\varphi(x),i=\varphi(y)$,那么就意味着不存在 i,j 使得 $u_i=u_j=a$,并且 $j-i=l$. 所以,当 $l\in\varphi(M)$ 时,有

$$\{u_i:u_i=L^l(u)_i,u_i\neq e,i=0,1,\cdots,q^2-2\}=\varnothing.$$

进一步,考虑 $a=e$ 的情况,此时 $\{i:u_i=e\}=\varphi(D)\cup\varphi(E)$. 根据 E 的定义 $E=\{x\in F_{q^2}^*:\mathrm{Tr}_{q^2/q}(x)=0\}$,所以存在 F_{q^2} 中的元素 θ,使得集合 $E=\theta F_q^*=\theta M$. 进而 M 中的元素总是可以表示成 E 中某两个元素的商. 这样一来,类似前面的讨论,有

$$\{u_i:u_i=L^l(u)_i,i=0,1,\cdots,q^2-2\}=\{e\}.$$

这样就完成了证明.

回顾 CACH 系统的定义以及(1)式,不难发现,序列 u 与其自身循环移位所产生的序列所构成的集合,已经具有非常接近于 CACH 系统所提出的要求. 其主要问题在于当 $l\in\varphi(M)$ 时,u 和 $L^l(u)$ 的交汇性很差. 下面证明通过 u 构造出一个新的 CACH 系统. 该系统是本文的主要结果.

定理 2 设 q 和序列 u 如定理 1 中定义. 对于 $j=-\lfloor(q+1)/2\rfloor,\cdots,-1,0,1$,序列 $v^{(j)}$ 定义为

$$v_i^{(j)}=\begin{cases}u_k, & i=2k;\\ u_{k+j}, & i=2k+1.\end{cases}$$

那么序列集合 $H=\{v^{(j)}:j=-\lfloor(q+1)/2\rfloor,\cdots,-1,0,1\}$ 构成一个 CACH 系统.

证明 首先,将 $v^{(j)}$ 记为 $v^{(j)}=[u,L^j(u)]$,这里 $[\cdot,\cdot]$ 的第一部分表示 $v^{(j)}$ 的偶数位元素 $(v_0^{(j)},v_2^{(j)},\cdots)$ 依次构成的序列,第二部分表示 $v^{(j)}$ 的奇数位元素 $(v_1^{(j)},v_3^{(j)},\cdots)$ 依次构成的序列. 对于任意的非负整数 l,$L^l(v^{(j)})$ 可以表示为

$$L^l(v^{(j)})=\begin{cases}[L^k(u),L^{k+j}(u)], & l=2k;\\ [L^{k+j}(u),L^{k+1}(u)], & l=2k+1.\end{cases}$$

进而对于任意的 $s,t\in\{-\lfloor(q+1)/2\rfloor,\cdots,-1,0,1\},s<t$,考虑跳频序列 $v^{(s)}$ 和 $v^{(t)}$ 的盲交汇性质. 对于任

意的非负整数 l，

$$\{v_i^{(s)}:v_i^{(s)}=L^l(v_i^{(t)})\}=\begin{cases}\{u_i:u_i=L^k(u)_i\}\cup\{u_i:L^s(u)_i=L^{k+t}(u)_i\}, l=2k,\\ \{u_i:u_i=L^{k+t}(u)_i\}\cup\{u_i:L^s(u)_i=L^{k+1}(u)_i\}, l=2k+1.\end{cases}\tag{2}$$

下面根据 l 的奇偶性，分两种情况来讨论.

(a) $l=2k$：若 $k\notin\varphi(M)$，即：$k\notin\{i(q+1):i=0,1,\cdots,q-2\}$，那么由定理 1 可知(2) 式此时等于

$$\{v_i^{(s)}:v_i^{(s)}=L^l(v_i^{(t)})\}\supseteq\{u_i:u_i=L^k(u)_i\}=M,$$

即：序列 $v^{(s)}$ 和 $L^l(v^{(t)})$ 交汇在所有的信道上.

若 $k\in\varphi(M)=\{i(q+1):i=0,1,\cdots,q-2\}$，那么由 $0<t-s<1+\lfloor(q+1)/2\rfloor<q+1$，有 $k+t-s\notin\varphi(M)$，进而

$$\{v_i^{(s)}:v_i^{(s)}=L^l(v_i^{(t)})\}\supseteq\{u_i:L^s(u_i)=L^{k+t}(u)_i\}=M.$$

所以序列 $v^{(s)}$ 和 $L^l(v^{(t)})$ 总能交汇在所有的信道上.

(b) $l=2k+1$：若 $k+t\notin\varphi(M)=\{i(q+1):i=0,1,\cdots,q-2\}$，那么由定理 1 可知(2) 式此时等于

$$v_i^{(s)}:v_i^{(s)}=L^l(v_i^{(t)})\}\supseteq\{u_i:u_i=L^{k+t}(u)_i\}=M,$$

即：序列 $v^{(s)}$ 和 $L^l(v^{(t)})$ 交汇在所有的信道上.

若 $k+t\in\varphi(M)=\{i(q+1):i=0,1,\cdots,q-2\}$，那么由于 $-1<-(s+t)<q+1$，有 $k+t+1-(s+t)\notin\varphi(M)$，进而

$$\{v_i^{(s)}:v_i^{(s)}=L^l(v_i^{(t)})\}\supseteq\{u_i:L^s(u_i)=L^{k+1}(u)_i\}=M,$$

所以此时序列 $v^{(s)}$ 和 $L^l(v^{(t)})$ 仍旧能够保证在所有的信道上交汇.

不难看出，定理 1 中所构造的 CACH 系统 H 总共包含了 $\lfloor(q+1)/2\rfloor+2$ 条序列，其周期为 $2(q^2-1)$，总共使用的信道个数为 $q-1$. 如果令 $N=q-1$，那么该系统 H 的周期接近 $2N^2$，而包含了 $\lfloor(q+1)/2\rfloor+2$ 条序列. 与例 1 中构造的完美 CACH 系统相比较，其周期增加了一倍，但是可用的序列数量增加了很多. 这样一来，该系统虽然完成的最短交汇时长比完美 CACH 系统要长，但是由于序列总数大大增加，因此可以支持很多次级用户同时使用该系统，进而比完美 CACH 系统有更强的实用性.

3　结束语

本文利用设计理论中经典的相对差集，对于任意的素数幂 q，构造出了一类新的完备的非同步跳频序列系统. 该系统使用 $q-1$ 个信道，构造的 CACH 系统 H 总共包含了 $\lfloor(q+1)/2\rfloor+2$ 条序列，该系统的序列周期长度已经非常接近最优的非同步跳频序列系统，与已有构造的完美 CACH 系统相比较，其周期大约增加了一倍，但是可用的序列数量大大增加了. 因此，通过这个新的 CACH 系统，更容易设计无线电交汇中非同步盲通信的协议或者算法.

参　考　文　献

[1] Bian K, Park J M. Asynchronous channel hopping for establishing rendezvous in cognitive radio networks[C]. 2011 Proceedings IEEE, Shanghai, 2011.

[2] Bian K, Park J M. Maximizing rendezvous diversity in rendezvous protocols for decentralized cognitive radio networks[J]. IEEE Transactions on Mobile Computing, 2013, 12(7): 1294-1307.

[3] Chen X, Zhou Y. Asynchronous channel hopping systems from difference sets[J]. Des Codes Cryptogr, 2016. DOI 10.1007/s10623-016-0221-8.

[4] Wu-K, Han F, Han F, et al. Rendezvous sequence construction in cognitive radio ad-hoc networks based on difference sets[C]. 2013 IEEE 24th International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), London, 2013.

[5] Gu Z, Hua Q S, Wang Y, et al. Nearly optimal asynchronous blind rendezvous algorithm for cognitive radio networks[C]. 2013 10th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), New Orleans, 2013.

[6] Beth T, Jungnickel D, Lenz H. Design theory. Vol. I, volume 69 of Encyclopedia of Mathematics and its Applications[M]. Cambridge: Cambridge University Press, 1999.

[7] Bose R C. An affine analogue of Singer's theorem[J]. J Indian Math Soc (N. S.),1942,25:171-183.

[8] Elliott J E H, Butson A T. Relative difference sets[J]. Illinois Journal of Mathematics,1966,10(3):517-531.

A New Family of Asynchronous Channel Hopping Systems Based on Relative Difference Sets

PAN Hongyan[1], FU Shaojing[2], DU Jiao[3]

(1. Department of Basic, Changsha Commerce and Tourism College, Changsha 410004, China;
2. Computer College National University of Defense Technology, Changsha 410073, China;
3. College of Mathematics & Information Science, Henan Normal University, Xinxiang 453007, China)

Abstract: In cognitive radio networks, to communicate with each other, two secondary users have to first establish links through a common channel, which is called a rendezvous. One solution to this challenging problem is to use a rendezvous protocol or algorithm based on a complete asynchronous channel hopping system, which plays a very important role in their design. In this paper, using relative difference sets from the combinatorial design theory, we propose a new CACH system for any prime power q, in which there are totally $q-1$ channels and $\lfloor (q+1)/2 \rfloor + 2$ sequences of a common period $2(q^2-1)$. Compared with the optimal CACH system, the sequence period of our new system is already very close to the optimal case, and it has more sequences. Hence, our new CACH system is more practical for designing new rendezvous protocols.

Keywords: channel hopping system; sequence period; relative difference sets

(上接第 169 页)

Prediction Model for Three-parameter Interval Grey Number Based on Kernel and Degree of Accuracy

LI Ye, ZHU Shanli, HOU Xianmin

(College of Information and Management Science, Henan Agricultural University, Zhengzhou 450002, China)

Abstract: Modeling objects of traditional prediction models are only suitable for real number sequences and interval grey number. Therefore, based on three-parameter interval grey number, and a new prediction model is proposed. The kernel sequences, the "center of gravity" sequences and degree of accuracy sequences are defined and predicted. Then the unbiased prediction model of three-parameter interval grey number is achieved by deducing and reverting. An example is presented to illustrate the usefulness and effectiveness of the proposed prediction method.

Keywords: grey system; prediction model; kernel and degree of accuracy; three-parameter interval grey number