计数式 TOD 跳频码发生器算法的构造 [1]

张申如 梅文华 * 王庭昌 **

(解放军理工大学理学院 南京 211101)
*(北京航空工程技术研究中心 北京 100076)
**(总参第 63 研究所 南京 210016)

摘 要 为同步长周期的跳频码序列，必须使用实时时间 TOD．一种新的眼光是将跳频码发生算法看作是对 TOD 这一特殊“信息”序列的“分组加密“变换．单调递增的计数式 TOD 是目前常用的 TOD 序列形式，然而，现有的跳频码发生算法并不适应长周期、单调递增计数式 TOD 的使用，该文讨论了分析、改造跳频码序列发生算法使之适合长周期单调递增计数式 TOD 的需求、又保持良好跳频特性这一重要任务．

关键词 跳频通信，码发生器，算法，实时时间
中图号 TN973.3

1 引 言

跳频通信是一种重要的通信抗干扰手段，通信双方使用相同的跳频码发生器，并使用相干检测等方法实现收发双方跳频序列在时间上的同步．跳频码的性能，对跳频通信系统的性能有重大影响，通常要求设计出来的跳频码序列族具有足够多的序列数，各序列平衡，线性复杂度高，并有良好的汉明自相关和互相关特性．跳频序列的设计，又必须考虑收发双方的同步方式．从快速同步角度考虑，跳频序列的周期不宜过长；为了不让敌方根据以前发射的频率信息方便地预测出下一个频率，又要求序列具有很长的周期，至少在 24 小时内不重复．例如 80 年代报道的 AN/URC-78[1] 和 SINCGARS- V [2] 甚高频跳频电台，序列周期就已达到了 $2^{32}-1 \approx 4.3\times10^9$．周期如此长的跳频序列，对每秒 500 跳左右的中速跳频，完成一个全周期的跳频大约需要 100 天．因此，在一次通信中，用户实际使用的跳频序列，仅仅是整个序列周期中很短的一部分．接收方如何凭借发送方的地址 (或共同的密钥) 做到与这一段跳频序列同步呢？这就需要使接收方获得发送方的初始状态矢量来决定自己跳频码发生器的初始状态．这个初始状态矢量通常称为实时时间 (TOD， Time of Date，又称跳历)．美国 AN/URC-78， SINCGARS- V 甚高频跳频电台， Falcon II 甚高频跳频电台，以色列 PRC-710 跳频电台，都使用了 TOD．尽管跳频码发生器已广泛使用了 TOD，但我们迄今尚未见到论述 TOD 定义及与跳频码发生算法关系的文章报道．

我们将在本文第 2 节描述 TOD 的定义和常见的两类 TOD 形式，并用新的眼光叙述了使用 TOD 跳频码发生算法的构成；第 3 节分析了现有的跳频码发生算法，着重研究了算法与计数式 TOD 相适应所存在的问题；第 4 节则针对宽间隔跳频码发生算法讨论了如何适应计数式 TOD 序列的要求；第 5 节叙述了使用 TOD 跳频码发生算法序列的周期定理和引理；最后给出了结论．

2 使用 TOD 的跳频码发生算法构成

在使用 TOD 的跳频码发生器中， TOD 决定着状态机的初始状态，状态机的状态随时间的变化形成 TOD 序列流．根据不同的同步方法，目前通常选择两种类型的状态机：一种是移位寄存器式 TOD，另一种是计数式 TOD．

[1] 2000-10-08 收到， 2001-03-06 定稿
成都电子科技大学战术通信抗干扰技术国防科技重点实验室项目基金和复旦大学专用集成电路国家重点实验室访问学者基金资助

对于移位寄存器式 TOD，线性或非线性反馈移位寄存器的实时状态矢量就是 TOD 序列的信息 [1,2]，再通过某种变换将 TOD 信息映射到跳频频隙集合上，就形成了跳频序列，详见图 1．在这种方案中，为实现收发同步，发送方必须将自己的 TOD 初值或序列的当前值，用规定的地址码调制后，通过勤务信道或者插入信息帧中发送出去，接收方则使用接收实时的 TOD 值来设置自己的线性或非线性反馈移位寄存器．

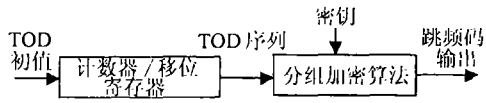

图 1　从 TOD 到跳频码输出

计数式 TOD 是目前比较通用的方案 [3−5]．它的 TOD 初值是由用户在按压跳频电台 PTT (Press To Talk) 键的实际时间按一定数据格式转换得到的二进制数字，TOD 序列就是从此时开始的实际时间按跳频码速映射的单调递增的数字序列．这种方案的优点是便于用高稳定和高精度的时钟取得、保持和调整同步．这也就是说，网内接收者 (即便是后入网的新用户) 就能够在一开始凭借时钟近似地逼近发送方跳频码发生器的实时状态；如果初始时，收发双方各自认定的时间有差异，接收方也便于通过慢 (快) 扫描或等待搜索的方法来取得同步信号中的 TOD，用以调整自己的 TOD 值，并在继后通信中一段很长的时间内保持同步．

对 TOD 序列而言，跳频码产生算法应有这样的性质：发送方从任何初始的 TOD 起，在后续的任一个时刻 TOD 产生的跳频码，与接收方直接注入该后续时刻 TOD 作初值所产生的跳频码完全相同．然而，对使用计数式 TOD 序列的跳频码发生器，接收方可独立地凭借通用时钟直接读该后续时刻的时间来产生 TOD 状态，他不必如使用移位寄存器式 TOD 那样，须从原有的初始 TOD 时刻起经状态机迭代演变到该后续时刻．

跳频码的产生唯一地决定于当前的 TOD 状态，对在此之前时刻 TOD 状态的无记忆特性，决定了对 TOD 序列流中每一个 TOD 值而言，这种跳频码产生方式是“分组”的．Diffie 和 Hellman[6,7] 曾给出一种同步流密码中密钥流的产生方法，用计数器流输出提供给一个分组加密算法作为输入来完成密钥流的产生．该方法也较好地描述了上述使用实时时间映射单调递增式 TOD 跳频码发生算法的构成．这里，TOD 的初值决定了计数器的初始状态，计数器的输出形成 TOD 序列流．实际上，上述两种状态机中跳频码的产生，都可看作是对 TOD 这一特殊“信息”流序列的“分组”加密映射变换 (图 1)，区别在于 TOD 序列的得到方式不同．

根据上面的叙述，可以归纳为：

TOD 序列的定义　在跳频码发生器中，由实际时间映射的用二进制矢量表示的数字序列流．它从初始的 TOD_0 值起，经有限状态机迭代连续产生．序列的循环周期 T 由表示 TOD 的字长 (字长通常会超过或远大于 32) 和所用的状态机决定，即表示为

$$\{\mathrm{TOD}_i, i = 0, 1, 2 \cdots | \mathrm{TOD}_i \in [0, 1, \cdots T-1]\}$$

TOD 序列的产生

移位寄存器式 TOD 序列的产生　$\mathrm{TOD}_i = f^i(\mathrm{TOD}_0)$, $f^i(\alpha)$ 为对状态 α 的 i 次迭代映射．

计数式 TOD 序列的产生　$\mathrm{TOD}_i = \mathrm{TOD}_{i-1} + \Delta \bmod T$, $\Delta = 1, 2, \cdots$, 增量 Δ 通常为 1．

从 TOD 到跳频码的产生　$C_i = H(\mathrm{Key}, \mathrm{TOD}_i)$, $H(,)$ 为在密钥 Key 控制下将 TOD 向跳频码空间映射的函数．

3 使用两类 TOD 的跳频码发生算法

跳频码的发生过程，可分为 TOD 序列的产生和对 TOD 序列的分组加密变换．可以用这个

新眼光，对现有的各种跳频码发生算法进行重新审视、分类.

所有类似于有限状态机的迭代算法，原则上都适合作为 TOD 序列的生成算法. 其中最主要的当然是线性 (或非线性) 反馈移位寄存器. 目前比较著名的，以有限域 GF(p) 或其扩域 GF(p^n) 中本原元的幂为基础序列的生成算法，如 m 状态抽样序列， L-G 模型， RS 序列， Bent 序列等 [8]，都是以 m 序列作为 TOD 序列，算法中后半部分描述的抽样和变换 (前馈) 处理都可看作是对 TOD 的分组加密. 由于这些 TOD 序列来源于时钟控制下迭代过程中的状态演变，每一个 TOD(即当前状态) 都依赖于前一个在自然序上通常并不直接相连的状态，所以，接收方、尤其是迟入网的用户，只能从发送方来得到即时状态. 要说明的是，这类算法本身已是 TOD 序列流产生加上从 TOD 序列产生跳频码的一个完整算法，因而作为一个整体，它不能再直接充当计数式 TOD 方案中的分组加密算法.

以 L-G 模型为例，参见图 2，它通过连续或非连续抽头，将 n 级移位寄存器的状态位与用户地址寄存器中的地址位进行位 "异或"，产生具有最佳汉明相关性能的跳频码序列族. 其良好的汉明相关性能来源于 m 序列良好的自相关特性. 然而，当我们要增大序列的周期，采用了很长的移位寄存器，又以计数式 TOD 序列作为移位寄存器的初始状态，这时 L-G 模型中的移位寄存器只能通过迭代适当轮次，充当一个分组加密器来加密 TOD 序列值，其状态输出与用户地址位 "异或" 后作为跳频码. 由于计数式 TOD 序列通常就像量化的 "时间流" 以均匀加 1 的计数器方式递增，它们在 m 状态序列中的位置是不均匀的，再作一定轮次的迭代，相当于对 m 状态序列作间隔不均匀的抽样，"跳跃式" 抽样序列常常丧失了原 m 状态序列或均匀抽样的 m 状态序列所具有的最佳自相关特性 (一种极端的特殊情况可帮助我们理解这一点，若迭代轮次设为零，输出的状态序列即为，从初始 TOD 开始均匀加 1 的递增序列，该序列的相关特性显然很差). 所以这个模型的整体不能 (至少不能直接这样) 在计数式 TOD 跳频码发生器中充当加密算法. 实际上，现有跳频码产生中类似以有限域 GF(p) 或其扩域 GF(p^n) 本原元的幂为基础序列的算法都如此，不能将它们整体地充当分组加密器应用于计数式 TOD 流序列.

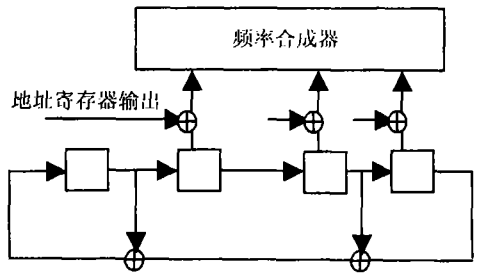

图 2 构造最佳跳频序列族的移位寄存器的 L-G 模型

然而，现也有一部分跳频码发生算法 [8] 是可看作能适应计数式 TOD 类型的，它们通常是基于素数 p 的有限域 GF(p)，并且以元素的升阶或降阶 (与计数式 TOD 序列特性吻合) 为基础的序列. 现仅举一例.

例 1[8] 基于有限域 GF(p)，使用频隙数目为 p，提供 $p-1$ 个一次重合序列，序列长度为 $L=p$，具体构造步骤为：(1) 选择一个素数 p；(2) 将 GF(p) 上的元素以升阶或降阶列出，如 $G=\{0,1,2,\cdots,p-1\}$；(3) 将 G 中各元素同乘以某一非零域元 u，就可产生一个非重复跳频序列，序列为 $S_u=\{s_u(j)=uj, j=0,1,\cdots,p-1\}$，式中，乘法以模 p 运算. (4) 通过乘以不同的非零域元，共可得到 $p-1$ 个非重复跳频序列 (Linear Congmence Code, LCC 码序列族).

在该构造方法中，用户的地址码序列为 u， TOD 序列就是计数器产生升阶排列的 p 个元素， $s_u(j)=uj \bmod p, j=0,1,\cdots,p-1$ 就是计算任何一个 TOD 对应的跳频码分组算法. 但

是，该算法由于频隙数目，序列周期， TOD 序列可取值数目都为 p ，频隙数目 p 通常过小，从而限制了它们的应用．所以，寻找一个分组算法，它能将字长通常达 40~128 位二进制矢量表示的计数式 TOD 序列，在长密钥 (字长通常超过 32 位) 下加密变换成性能良好、对应频隙数不大 (通常在 64~1024 范围内) 的跳频码序列是一个极重要的研究问题．

4 可使用计数式 TOD 序列的宽间隔跳频码发生算法

宽间隔跳频中也有同样的问题．跳频通信通常有两类实现宽间隔的方法：一类是着眼于频隙分配的算法，码的产生仍同于以往非宽间隔的算法；另一类是构造特定的宽间隔跳频码序列算法．

着眼于频隙分配的算法在使用计数式 TOD 序列时，跳频码的发生当然必须是第 3 节中指出的基于计数式 TOD 序列的算法．例如，去中间频带法 [8] 在划去了中间频带后，将可使用的频段分为上下两部分，由于预先可指定每个码元按计数式 TOD 的奇偶相间地对应上下两个频段中的一个频隙，所以原则上仍可用来产生增量为 1 的计数式 TOD 宽间隔跳频码．然而，另一些分配频隙的算法却会受到 TOD 引入的限制，如对偶频带法 [8] ，它是将当前码与前一个码进行比较来决定是否跳入对偶频带．由于算法中当前跳频码对应的频隙还依赖于前一个跳频码对应的频隙，与当前 TOD 之间的关系并不确定，因而就不能使用在带 TOD 的情况．因为不同的 TOD 起始将可能导致在时间流动中同一 TOD 的跳频码对应的频隙不同．

直接构造宽间隔跳频码的算法也是如此，例如下述算法，仍可用于构造计数式 TOD 序列的宽间隔跳频码．

例 2[8]　使用频隙数目 q 为素数，能得到 $q-2d-1$ 个长度为 $L=q$ 间隔为 d 的一次重合宽间隔跳频码序列，具体构造步骤为：(1) 设频隙数目 q 为素数；(2) 将 GF(q) 上的元素以升阶或降阶列出，如 $G=\{0,1,2,\cdots,q-1\}$；(3) 将 G 中各元素同乘以某一非零域元 $u(d+1\le u\le q-d-1)$，就可产生一个非重复宽间隔跳频序列，序列为 $S_u=\{s_u(j)=uj, j=0,1,\cdots,q-1\}$，式中，乘法以模 q 运算．(4) 通过乘以不同的非零域元 u, $d+1\le u\le q-d-1$，共可得到 $q-2d-1$ 个一次重合的宽间隔跳频序列．实际上该码序列族是例 1 中 LCC 码序列族的一部分．

在该构造方法中，用户的地址码序列为 u， TOD 序列就是升阶排列的 q 个元素，计算任何一个 TOD 对应的跳频码就是对当前 TOD 值的变换．

经我们分析研究，任何使用增 1 计数式 TOD 序列的跳频码发生算法，都可以按图 3 所示的方法改造成宽间隔跳频码序列的发生算法 [9] ．

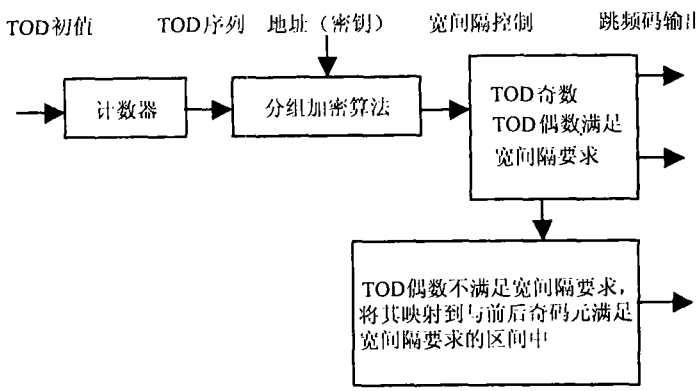

图 3　从增 1 计数式 TOD 到宽间隔跳频码输出

该方案中，对原分组加密算法得到的跳频码，当 TOD 为奇数 (也可偶数，若偶数的话，下面叙述的奇偶反过来，该控制算法的核心是实现宽间隔又切断码元间过长的关联) 时直接输出；当 TOD 为偶数时，分两种情况：与前后两个码元相比，若满足宽间隔要求，也直接输出，若不满足要求，则利用当前 TOD 加密成的另一随机数将其映射到与前后两个奇 TOD 码元满足宽间隔要求的区间中去．显然，这个控制算法中每一步都需要在存储器中保存前后两个 TOD 对应的跳频码元．

由于算法中确立了奇 TOD 对应的跳频码不加变动而直接输出，偶 TOD 对应的码元若与前后两个奇 TOD 对应码元不满足宽间隔要求时，它也被当前 TOD 唯一确定地加以映射．每一个跳频码元至多与前后两个码元相关联，这两个被关联的码元又仅与它们自己的 TOD 唯一对应，不再波及其它码元，因而就能从中间任一 TOD 起始来产生跳频码序列．

5 使用 TOD 的跳频码发生算法序列的周期

对使用 TOD 的跳频码发生算法序列的周期，我们有如下的定理和引理．

定理 1 使用 TOD 的跳频码发生算法，跳频码的周期不会长于产生 TOD 的状态机序列的周期 (范围)．

这一定理的证明从图 1 的结构看是明显的，由于仅对 TOD 实施了分组加密映射，当 TOD 输出在一个周期后重复时，跳频码必然重复输出．定理得证．

这个定理的重要性在于告诉我们，使用实时时间 TOD 的跳频码发生算法时，若要增长跳频码的周期，应尽可能选用较长周期的 TOD 序列生成算法，采用大字长的线性反馈移位寄存器和增 1 计数器作状态机就是如此．分组加密算法的选用还应保证跳频码的周期保持为状态机的周期．一旦达到此限，跳频码的周期不会再随分组加密算法中密钥字长的增加而增长，密钥字长增长可用来增多用户数．使用计数式 TOD，对于增量有下述引理．

引理 1 计数范围在 $0,1,\cdots,q-1$ 的计数器，对于满足 $(\Delta,q)=1$ 计数增量 Δ，跳频码的周期不变．

证明 令 TOD_0 为 TOD 的初值，由于 $\mathrm{TOD}_m=\mathrm{TOD}_0+m\Delta \bmod q$，$m$ 为增加的次数，根据同余理论，当且仅当 $(\Delta,q)=1$，在 m 跑遍 $0,1,\cdots,q-1$ 的计数范围时，TOD_m 将跑遍 $0,1,\cdots,q-1$ 的计数范围． 证毕

这个引理重要性在于告诉我们，为了不缩短跳频码的周期，除了可选择增量 $\Delta=1$ 以外，还可以选择与 q 互素的增量，例如对 $q=2^r, r=2,3,\cdots$，我们可以选择非偶数的 $\Delta=3$ 等，这样用户的跳频码将以不同的次序跑遍其周期．但若增量 Δ 选择为偶数，则会使跳频码的周期缩短，例如 $\Delta=2$，跳频码的周期减半．

6 结束语

为同步长周期的跳频码序列，必须使用实时时间 TOD．跳频码的发生实际上可看作是对 TOD 这一特殊“信息”序列的“分组”加密变换．单调递增计数式 TOD 是目前常用的 TOD 序列形式．用这种从 TOD 序列到跳频码序列的新模型考察现有的各种跳频码产生算法 (包括宽间隔跳频在内)，其中大量以有限域 $\mathrm{GF}(p)$ 或其扩域 $\mathrm{GF}(p^n)$ 本原元的幂为基础序列的算法，都不宜直接将算法的整体来充当计数式 TOD 序列的分组加密器．部分符合计数式模型的跳频码发生算法也有周期过短的弱点．慎重地分析，改造已有的跳频码序列产生算法，开发新的序列构造方法，使之适合长密钥控制下，对极长周期计数式 TOD 输入变换的需求，又保持良好跳频特性是十分重要的．

参 考 文 献

[1] 施国楠，AN/URC-78 电台电子抗干扰控制系统的主要硬件功能，军事通信技术，1981 年增刊《野战通信抗干扰技术学术讨论会文选 (下集)》，14-22.

[2] 倪君生，慢跳频网同步的建立，军事通信技术，1980, (2), 30-36.

[3] 姚富强，邹敏之，战术微波接力机抗干扰设计，军事通信技术，1994, (3), 33-37.

[4] 陈建忠，短波模拟跳频电台数字同步系统的工程实现，现代军事通信，1995, 3(1), 49-54.

[5] 赖仪一，数字短波跳频电台跳频图案的设计，现代军事通信，1996, 4(3), 41-46.

[6] W. Diffe, M. Hellman, Privacy and authentication: an introduction to cryptography, Proc. IEEE, 1979, 67(3), 394-427 .

[7] M. E. Hellman, On DES-based synchronous encryption, Dept. of Electrical Eng., Stanford University, Stanford, Calif., 1980.

[8] 梅文华，杨义先，跳频通信地址编码理论，北京，国防工业出版社，1996, 85, 159.

[9] 何维苗，应用混沌理论产生宽间隔跳频码序列，[硕士论文]，南京通信工程学院，1998, 5.

CONSTRUCTION OF ALGORITHM FOR FREQUENCY HOPPING CODE GENERATOR USING COUNTING TOD

Zhang Shenru　Mei Wenhua*　Wang Tingchang**

(*Inst. of Science, PLA University of Sci. and Tech., Nanjing* 211101, *China*)

*(*Beijing Aeronautical Technology Research Center, Beijing* 100076, *China*)

**(*The 63th Institute of PLA General Staff, Nanjing* 210016, *China*)

Abstract It is necessary to use the reference real time TOD(Time Of Date) for synchronizing a hopping sequence with long period. There is a new view that the generation of hopping codes is a process in which the special information sequences TOD are translated by a block encoding. Today monotonously increasing TOD is a common form, but there are collides between existing generating algorithm of hopping code and monotonously increasing TOD with long period. A important task of study on generating algorithm of hopping code which is suitable for monotonously increasing TOD with long period and keeps good properties is discussed in the paper.

Key words Frequency hopping communication, Code generator, Algorithm, Time Of Date (TOD)

张申如：　男，1946 年生，教授，感兴趣的领域有光电信息处理、扩展频谱通信及专用集成电路设计等.

梅文华：　男，1965 年生，高级工程师，工学博士，中国电子学会高级会员、青年工作委员会委员、可靠性分会委员，感兴趣的领域有扩展频谱通信、最佳编码信号设计、可靠性增长等.

王庭昌：　男，1943 年生，研究员，中国电子学会通信专业委员会委员，感兴趣的领域有语音压缩、混沌信号处理及专用集成电路设计等.