文章编号:1671-6833(2006)02-0110-03

三元树上的线性递归序列

王锦玲,毕文斌

(郑州大学数学系,河南 郑州 450052)

摘 要:利用图论中的三元树理论将GF(2)上的一类钟控序列构造成GF(3)上的最长游程仅为2的序列,从而获得了一个线性复杂度更高,随机性更强的新序列.

关键词:线性复杂度;周期;三元树;钟控序列;随机性

中图分类号:O 151;O 157.6 **文献标识码**:A

0 引言

线性复杂度及伪随机性是衡量流密码安全性的两个主要指标,T. Beth所给出的停-走(钟控)序列在提高线性复杂度方面较为理想,但由于长游程过多过长,伪随机性较差.本文将流密码理论与图论中的三元树理论相结合,从而将原序列的线性复杂度($n(2^n-1)$)提高一个量级($c(2^n-1)^2$),由于最长游程为2游程,所以伪随机性更为理想.

1 关于停-走序列的定义及基本结论

定义 设GF(2)上两个n级m-序列为

$$a^\infty = a_0a_1a_2\cdots;\ b^\infty = b_0b_1b_2\cdots$$

它们的极小多项式分别为$f(x)$和$g(x)$.整数函数$G(t)$为

$$G(0)=0;\ G(t)=\sum_{i=0}^{t-1}a_i,\ t=1,2,\cdots$$

定义停走序列$u^\infty = u_0u_1u_2\cdots$为:$u_t = b_{G(t)}$,$t=1,2,\cdots$

定理 停走序列u^∞的极小多项式为$g(2^{n-1})$,线性复杂度为$n(2^n-1)$,最小周期为$(2^n-1)^{2[2]}$.

2 生成一棵特殊的有序三元树

我们要造一棵有16片叶子的有序三元树(关于有序三元树的定义及编码方法见参考文献[4]),它须满足条件:

(1) 这16片叶子的任一片的编码必须满足3个条件:①编码的前两位数字不同;②编码的后两位数字不同;③除第一位和最后一位,中间的数字至多为二游程.

例如:允许的编码:012,0112;不允许的编码:110,011,01112.

(2) 这16片叶子的编码中,0,1,2出现的概率应尽量保持均等.

我们依条件(1)、(2)生成一棵有序三元树T,并以图1为例做以后的分析.

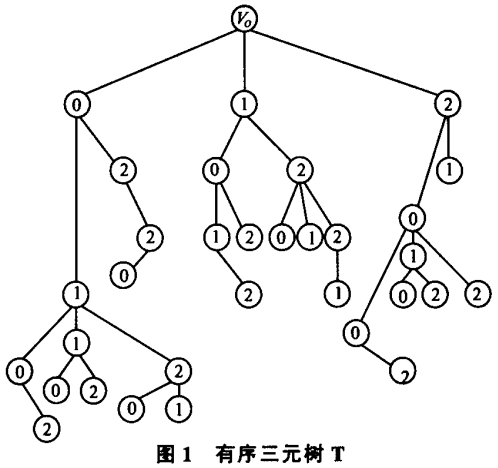

图1 有序三元树T

Fig.1 Orientted triael-tree T

这16片叶子的编码依次为:0102,0110,0112,0120,0121,0220,1012,102,120,121,1221,2002,2010,2012,202,21.

易知,这些符合条件(1),在这些编码中,0,1,2分别出现19次,19次,20次,所以也符合条件(2).

收稿日期:2005-11-25;**修订日期**:2005-01-18

基金项目:河南省自然科学基础研究计划项目(200510459003)

作者简介:王锦玲(1963-),女,河北安国人,郑州大学副教授,主要从事代数密码方面的研究.

3　将停－走序列 u^∞ 构造成 GF(3) 上的新序列 v^∞

将停－走序列 u^∞ 从 u_0 开始，每 4 个数字为一组，即 $(u_0u_1u_2u_3)(u_4u_5u_6u_7)\cdots$，因为 $(u_iu_{i+1}u_{i+2}u_{i+3})$ 共有 $2^4=16$ 种情况，我们将每一种情况对应于有序三元树 T 的一片叶子，将 $(u_iu_{i+1}u_{i+2}u_{i+3})(i\geqslant 0)$ 变为对应叶子的编码，规定对应情况如下：

0000→0102　0001→0110　0010→0112
0100→0120　1000→0121　0011→0220
0101→1012　1001→102　0110→120
1010→121　1100→1221　0111→2002
1011→2010　1101→2012　1110→202
1111→21

因为 u^∞ 的周期为 $(2^n-1)^2$，且 $\gcd(4,(2^n-1)^2)=1$，所以 u^∞ 每经过 4 个周期，v^∞ 经过 1 个周期.

又由于我们对此树 T 有条件(1)的限制，所以 v^∞ 中游程至多为 2.

例　设 $n=2, g(x)=x^2+x+1$ 为 GF(2) 上的本原多项式，从而为 GF(2) 上的生成多项式，u^∞ 的周期为 9，线性复杂度为 6.

设 u^∞ 的初始向量为(010011)，则 u^∞ 的前 4 个周期为

u^∞:(0100)(1100)(1010)(0110)(0101)(0011)(0010)(1001)(1001)；

v^∞:0120　1221　121　120　1012　0220　0112　102　102

易知 v^∞ 的周期为 32，其中 0，1，2 出现的次数分别为 9 次，12 次，11 次，基本符合概率均等的目标.

4　v^∞ 的周期及线性复杂度分析

4.1　v^∞ 的周期分析

在这 16 片叶子中，编码为 4 位的有 11 片，3 位的有 4 片，2 位的有 1 片，假设它们以等概率出现，我们可以简单地估计 v^∞ 的周期：

$$T\approx\frac{11\times4+4\times3+1\times2}{16\times4}\times4\times(2^n-1)^2$$
$$\approx3.6(2^n-1)^2.$$

当 T 越大，即 n 越大，T 偏率 $3.6(2^n-1)^2$ 的相对幅度越小；

当 T 越小，即 n 越小，T 偏率 $3.6(2^n-1)^2$ 的相对幅度大；

这是因为 T 越大，叶子出现的概率越接近随机性，而 T 越小，偶然性就越大.

4.2　v^∞ 的线性复杂度分析

显然 v^∞ 是 GF(3) 上的一个周期序列，对其线性复杂度的分析，我们不能忽略 v^∞ 中不含长为 2 以上的游程这一因素.

假设 v^∞ 的周期为 T，线性复杂度为 m，当 m 较大时，任给一个不含长为 2 游程的初始状态，v^∞ 中很难避免出现 3 及 3 以上的游程.

下面我们考虑不出现 3 游程时，m 与 T 的关系：

假设 $T-m=i$，$v^\infty=v_0v_1v_2\cdots v_{m-1}v^m\cdots v_{T-1}v_0v_1\cdots$，$(v_iv_{i+1}v_{i+2})(i\geqslant m-2)$ 共有 $3^3=27$ 种情况，假设它们等概率地出现，则 $(v_iv_{i+1}v_{i+2})(i\geqslant m-2)$ 不是 3 游程的可能性为 $\frac{8}{9}$，所以 v^∞ 不出现 3 游程的可能性为

$$\left(\frac{8}{9}\right)^{T-m+1}=\left(\frac{8}{9}\right)^{i+1}.$$

i 取 38 时，

$$\left(\frac{8}{9}\right)^{i+1}=\left(\frac{8}{9}\right)^{39}\approx1\%.$$

换言之，当 $T-m=38$ 时，v^∞ 中出现 3 游程的可能性为 99%，从而 $T-m\geqslant38$ 的概率为 1%，即 v^∞ 的线性复杂度与周期相差不大，在 v^∞ 的一个周期 T 内，v^∞ 可视为随机序列.

5　v^∞ 的重量复杂度 $WG_k(v^\infty)$ 分析

将 v^∞ 中的 k 个 0 变为非零，得到的新序列记为 w^∞，我们假设这 k 个 0 的分布为最不理想的情况，即它们大致均匀地分布在 w^∞ 整个周期中，且这 k 个长游程均达到最大值 5，由抽屉原理：w^∞ 中至少有一段最长游程不大于 2 的序列，其长度 $l\geqslant\frac{T}{k}-5$. 若 $\frac{T}{k}\geqslant46$，由 4 中的分析，$T-m\geqslant38$ 的概率不超过 1%.

我们以一个实例来说明：通过改变 v^∞ 中的 0 来试图找出其极小多项式是不行的. 假设 $n=5$，则 v^∞ 的周期 $T\approx3.6(2^5-1)^2\approx3\,360$ 若想避免 w^∞ 中随机序列(最长游程不超过 2)的长度小于 41，则至少要改变 73 个 0. 这说明 v^∞ 具有非常优良的伪随机性.

6　结论

(1) 若敌手已知密文 v^∞，且知道这种密码体制，则他若试图找出产生 u^∞ 的极小多项式，他必

须确定 GF(2)上的 4 元与 16 片叶子的一一对应情况.但这样的一一对应共有 16! 种,所以敌手的这种目的极难达到.

(2) 一般情况下,可视明文长短来确定 n,使得明文长度 $l < T$.

参考文献:

[1] BETH T, PIPER F C. The stop-and-go generator[J]. Lecture Notes in Computer Science, 1985, 209: 88 ~ 92.

[2] 胡予濮,张玉清,肖国镇.对称密码学[M].北京:机械工业出版社,2002.

[3] 丁存生,肖国镇.流密码学及其应用[M].北京:国防工业出版社,1994.

[4] 王树禾.图论[M].北京:科学出版社,2004.

The Linear Recurring Sequence On Triad - tree

WANG Jin - ling, BI Wen - bin

(Department of Mathematics, Zhengzhou University, Zhengzhou 450052, China)

Abstract: By means of the triad - tree theory in graph theory, a sequence in GF(3) is transformed from a sort of clock control sequence in GF(2), and its longest pattern is no more than 2, its linear complexity is higher and its stochastic is more ideal.

Key words: linear complexity; period; triad - tree; clock control sequence; stochastic

(上接第 109 页)

参考文献:

[1] 王 纯,郭卓明,王 健.双提篮拱桥的设计与静力分析[A].中国公路学会.2005 年全国桥梁学术会议论文集[C].北京:人民交通出版社,2005.1035 ~ 1041.

[2] 钟铁峰,殷学纲,陈 淮.斜靠式异型拱桥体系振动特性分析[J],桥梁建设,2005,(2):8 ~ 11.

[3] 陈宝春.钢管混凝土拱桥设计与施工[M],北京:人民交通出版社,1999.

[4] 李广慧,刘晨宇,托拉·欧尼弗里奥.响应面方法及其在桥梁体系可靠度分析中的应用[J].郑州大学学报(工学版),2004,25(1):11 ~ 14.

The Design and Stability Analysis of Continuously Multi - span Slanting Arched Bridge

ZHANG Tian - hang, LI Qing - fu

(School of Environment and Water Conservancy, Zhengzhou University, Zhengzhou 450002, China)

Abstract: Slanting heterogeneous type arched bridge is a new type of space composite structure system with specific characteristics. this paper takes the HanJiang bridge as an example, introduces the continuously multi - spans slanting arched bridge design and the arrangement continuously, analyzes the bridge structure system characteristic, through the plane and the spatial static computation, indicates entire bridge structural design stress reasonable, arches the section, the suspension link, the tie bar, box beam, supports the concrete storage stress reserve to be moderate, each cross displacement satisfies the norm requirements; The main span power structure analysis calculates A, B, C three cross structure plane, outside the rigidity approaches, loses the steady modality to the 1st step to solve the critical load proportionality factor computed result to be bigger than 5 for the stability coefficient, the structure has a kind to lose the steady possibility to be small, and the spatial stability also meets the demands.

Key words: slanting arched bridge; static computation; stability computation