摘要

ABSTRACT

目录

第1章 绪论

第2章 混沌密码学的研究现状

第3章 基于混沌性态的离散动力系统的串编码

3.1 导论

3.1.1 术语约定

在计算机上，任何文件、文本实际上均为有穷二进制串，可以看作符号空间的一个序列。基于这个特点，本章将提出一种利用离散动力系统将二进制串进行编码的方案，并从数学上对其进行定义与证明。考虑更一般的情况，对于含有个符号的符号集，约定为由中元素组成的长度有限的序列的集合，那么由构成的符号空间、、，也存在一组一般的条件来构造具体的编码与解码过程。为节约篇幅，本章将直接简称离散动力系统为“动力系统”或“系统”，以“状态”指代动力系统在相空间的点。假设动力系统的映射为，且系统的当前状态与下一个状态存在递归关系

 (3.1.1)

由此得到序列，其中为初始条件，下标为系统的离散时间，是可逆的。为动力系统的状态集。编码的过程实质上为动力系统迭代的逆过程，而得到的编码结果即为解码时传入动力系统的初始条件。为方便叙述，现将一些术语约定如下

1. 选择条件：在编码过程中，动力系统的每个状态均对应符号空间的一个符号，该对应关系可用满射

 (3.1.2)

表示。由选择条件可知，仅依靠动力系统的状态即可演算出对应的符号，这也是解码的原理。

1. 状态组：有序对，包含动力系统的状态和符号集的一个符号，记作

 (3.1.3)

状态组集为后文二元函数的定义域，记作，有

 (3.1.4)

1. 回溯与选择性回溯：二者均为表示逆向迭代的过程，回溯得到的结果为动力系统的所有可能的前一个状态的集，称作回溯状态集，记为。选择条件和动力系统的选取应当使除不动点的状态回溯得到的且，此即后文提到的回溯条件。回溯过程定义为动力系统的状态集到状态集族**A**的一一映射

**A****A****P** (*S*) (3.1.5)

显然的对应法则是

**A** (3.1.6)

由于的陪域不包含于定义域，该映射无法递归。在编码过程中，除了当前状态还需要以符号作为参数求得满足选择条件的所有可能的前一个状态的集，此过程称作选择性回溯。选择性回溯得到的状态集称作选择性回溯状态集，记作。选择条件和动力系统的选取应当使除不动点外的状态选择性回溯得到的。显然，选择性回溯状态集存在以下性质



 (3.1.7)

选择回溯的定义如下

**A****A****P** (*S*) (3.1.8)

其对应法则是

**A** (3.1.9)

动力系统能够用于编码的条件是

 (3.1.10)

故集一定是在映射下的原像集的子集。式(3.1.10)称作回溯条件。将所有可能的组成集族B，根据选择公理，集族B上存在一个选择函数

B 。在一次回溯过程中，同一符号对应的回溯状态可能不止一个，需要从中选择一个状态，这个过程依靠选择函数完成。记选择的回溯状态为，回溯并选择的过程记作

 (3.1.11)

在编码过程中，状态和符号都是以序列的形式出现。若以状态和符号为参数回溯1次，记作

 (3.1.12)

为了递归地表示编码过程，在定义一个自映射，对应法则如下

 (3.1.13)

其中表示串的第个符号。如果为有穷串，则整个编码过程可以表示为

 (3.1.14)

意为从串的最后一位符号开始向前回溯。有穷串的编码对于实际应用已经足够。对于无穷串可以对称地构造一个双无穷序列，满足条件

 (3.1.15)

显然，每个有且只有唯一的一个满足以上条件。这样即可从开始向负方向回溯，设对编码得到的初始条件为。编码过程可表示为

 (3.1.16)

据解码得到的串与原串呈镜像对称关系。

1. 迭代结果：表示被编码的串。
2. 初始条件：表示编码得到的结果。理论上讲，不论是有穷串还是无穷串，其编码结果均可用系统的状态表示，这也表明数学上的动力系统编码实际上是压缩编码。

一个完整的编码系统，可由选择条件(3.1.2)与满足回溯条件(3.1.10)的动力系统定义。显然，能够用于编码的动力系统一定不存在逆映射，而定义动力系统的迭代映射也一定不是单射。同时，对除不动点外的状态回溯得到的回溯状态集和选择性回溯状态集的基的要求也应得到满足，如果状态为动力系统的不动点，那么上一个状态也就无法选择，编码系统将失效。在实际应用中，应当尽可能保证轨线在一个闭区域内，并且在该区域内发散，这样做是为了防止轨线发散到无穷或是收敛到不动点，甚至取得定义域外的回溯状态。能够用于编码的动力系统完全可以不具备混沌性态。

混沌性态的系统具有初始条件敏感性，初始条件的任何微小误差也将导致轨线在很快的时间内发散。同样，如果在已知初始条件的情况下，如果系统参数存在微小的误差，那么解码得到的串也将从某个有限位数开始与原串不匹配。通常情况下，对于有穷串，其初始条件为混沌映射定义域的一个子集，而无穷串的初始条件则可能只是单一的点。

编码的过程亦可视为一个加密过程，按照传统的密码学体系可以将这个加密系统的组成部分解释如下

1. 明文：作为动力系统的迭代结果的串。
2. 密文：动力系统回溯得到的初始条件。
3. 密钥：动力系统的系统参数。
4. 加密算法：动力系统回溯的过程。
5. 解密算法：动力系统迭代的过程。

在这个过程中，迭代或回溯的次数取决于串的长度。

对于一维的迭代映射为连续映射的数学混沌，明文集为，密文集为的一个子集。根据混沌系统的选用不同，作为密钥的系统参数极有可能存在等效密钥，尤其是定义于上的混沌系统。如果定义密钥空间为所有密钥组成的集合，那么该加密系统的密钥空间是连续统，而等效密钥空间却只是可数集。当然，这仅仅是数学上的理论情况，对于精度有限的计算机而言情况要糟糕很多，尤其是混沌特性的退化和精度限制导致的误差扩散。这将分别导致本该具有混沌性态的动力系统出现周期性和编码位数过短。

3.1.2 动力系统的状态

动力系统迭代得到的点叫做动力系统的状态。由于编码得到的结果也是系统的一个状态，因此有必要了解系统状态的性质。在动力系统中有几类特殊的点，

它们分别是周期点、不动点。它们取决于系统参数的取值。

3.2.1.1 动力系统的周期点

3.2.1.2 动力系统的不动点

3.3 基于Logistic混沌系统的一种编码与解码方案

3.3.1 数学混沌的理论证明

本节将采用Logistic映射作为混沌映射对上文提到的编码方案进行论证，证明使用的映射定义为

(3.2.1)

其中和为系统参数，在实际使用中可以作为密钥进行更改。在论证过程中，将直接采用原始符号进行证明，并且求出和需要满足的条件。

定义，由此得到序列，其中为初始条件，后续值依照该递归关系计算。由于该映射不存在逆映射，但使得成立的两个实数、有如下关系

(3.2.2)

为了方便叙述，作如下约定

假设，其中为正实数，为负实数，则有



 (3.2.3)

理论上讲，系统参数可以任意更改，只要系统参数符合临界条件。但由于64位浮点数精度有限，混沌特征可能退化，甚至出现周期性。理论上合法的和的值不一定会让程序产生正确的输出。通常情况下可取。初始条件可以随意变动，在上述通常系统参数取值的情况下，有。

明文每16位被加密成一个双精度浮点数，初始条件为，辅助处理函数的初始条件为，辅助函数将浮点数编码成字母序列。

过程：

1、编码明文的长度（64位无符号数），得到4个64位浮点数。选择