

文章编号:1008-1542(2012)01-0011-03

距离正则图相关联的两类认证码

岳孟田¹, 李增提²

(1. 廊坊师范学院科研处, 河北廊坊 065000; 2. 廊坊师范学院数信学院, 河北廊坊 065000)

摘要:利用了序为 (s, t) 的距离正则图和直径为 d 的对极的距离正则图构造了 2 类 Cartesian 认证码, 并且计算了它们的参数及模仿攻击成功的概率 P_1 和替换攻击成功的概率 P_s 。

关键词:距离正则图; 认证码; 团

中图分类号:O157.4 文献标志码:A

Two kinds of authentication codes associated with distance-regular graphs

YUE Meng-tian¹, LI Zeng-ti²

(1. Department of Science and Study, Langfang Normal College, Langfang Hebei 065000, China; 2. Department of Mathematics, Langfang Normal College, Langfang Hebei 065000, China)

Abstract: Two kinds of Cartesian codes are constructed by using a distance-regular graph of order (s, t) and antipodal distance-regular graphs of diameter d , respectively. Moreover, their parameters and the probability of successful impersonation attack and substitution attack are computed, respectively.

Key words: distance-regular graph; authentication code; clique

设 S, E 和 M 是 3 个非空有限集, $f: S \times E \rightarrow M$ 是一个映射, 且满足下面的条件:

1) 映射 f 是满射;

2) 对任给的 $m \in M$ 和 $e \in E$, 如果存在一个 $s \in S$, 使得 $f(s, e) = m$, 这样的 s 是被 m 和 e 所唯一确定的, 则称四元组 $(S, E, M; f)$ 是一个认证码。

设 $(S, E, M; f)$ 是一个认证码, S, E 和 M 分别称为信源集、编码规则集和信息集; f 称为编码映射。对 $s \in S, e \in E, m \in M$, 若 $m = f(s, e)$, 则称信源 s 在编码规则 e 下加密成信息 m , 或简单的说 m 包含编码规则 e , 也说 s 是相应于信息 m 的信源, 基数 $|S|, |E|$ 和 $|M|$ 称为这个码的参数。

在文献[1]—文献[5]中, 万哲先、高锁刚等已经利用有限典型群几何的子空间构造了认证码, 并计算了它们的参数和成功地模仿攻击和替换攻击概率。在本文中, 利用序为 (s, t) 的距离正则图和直径为 d 的对极的距离正则图构造了 2 类 Cartesian 认证码, 并且计算了它们的参数及模仿攻击成功的概率 P_1 和替换攻击成功的概率 P_s 。

1 距离正则图

关于距离正则图的概念及有关知识, 详见文献[6]。

收稿日期: 2011-09-06; 修回日期: 2011-11-20; 责任编辑: 李 穆

基金项目: 国家自然科学基金资助项目(10971052)

作者简介: 岳孟田(1973-), 男, 河北廊坊人, 副教授, 硕士, 主要从事代数组合方面的研究。

设 $\Gamma=(X,R)$ 是一个连通图,对于 X 中的任意 u 和 v ,设 $\partial(u,v)$ 表示 u 和 v 之间的距离,称 u 和 v 是邻接的,如果 $\partial(u,v)=1$,对于任意顶点 u ,设

$$\Gamma_i(u)=\{v\in X|\partial(u,v)=i\}.$$

Γ 的距离函数的最大值称为 Γ 的直径, X 的一个 l -子集 A 称为 Γ 的大小为 l 的团,如果 A 中任意的 2 个不同顶点是邻接的, X 的一个 l -子集 A 称为 Γ 的大小为 l 的 d -团,如果 A 中任意的 2 个不同顶点的距离是 d ,空集 \emptyset 规定是大小为 0 的团(或 d -团)。

设 $\Gamma=(X,R)$ 是一个直径为 d 的连通图,对任意整数 $h,i,j(0\leq h,i,j\leq d)$ 和所有 $u,v\in X$ 且 $\partial(u,v)=h$,若 $p_{i,j}^h=|\{w\in X|\partial(u,w)=i,\partial(w,v)=j\}|$ 是不依赖于 X 中 u,v 的选取,那么 Γ 叫做距离正则图。在这种情形下,对任意顶点 u , $\Gamma_i(u)$ 的基数仅依赖于 i 记作 k_i 。

$\Gamma=(X,R)$ 是一个距离正则图,若对于每个顶点 $u\in X$,诱导子图 $\Gamma(u)$ 都是 $t+1$ 个大小为 s 的团不交并,则 Γ 叫做序为 (s,t) 的距离正则图。因为 $\Gamma(u)=\{v\in X|\partial(u,v)=1\}$, W 是 $\Gamma(u)$ 中大小为 s 的最大团,那么 $W\cup\{u\}$ 是 Γ 中大小为 $s+1$ 的最大团,因此 Γ 中每个最大团都有 $s+1$ 个顶点,且每个顶点都包含在 $t+1$ 个最大团中。

一个直径为 $d(d\geq 2)$ 的距离正则图 Γ 称为对极的,若 $\partial(x,y)=\partial(x,z)=d$,则有 $y=z$ 或者 $\partial(y,z)=d$ 。

2 序为 (l,t) 距离正则图相关联的认证码

在此,假定 $\Gamma=(X,R)$ 是有 n 个点的序为 (l,t) 的距离正则图,设 C 表示 Γ 所有团的集合。

构作 I 设信源集 S 是 Γ 中的 $(t+1)l$ 点,对任意 $x\in X$,设 e_x 是一个从 S 到 $\Gamma(x)$ 的双射, $E=M=X$ 。对任意信源 s 和编码规则 x ,定义 $f(s,x)=e_x(s)$,那么 $(S,E,M;f)$ 是一个认证码。

定理 1 构作 I 的 $(S,E,M;f)$ 是一个认证码。

证明:

根据以上构作可知 $f(s,x)=e_x(s)$, $s\in S$, $x\in E$ 是一个映射,

对任意 $y\in M$,取 $x\in E$,可得到一个双射 $e_x:S\rightarrow\Gamma(x)$,那么存在 $s\in S$,使得 $e_x(s)=y$,所以 f 是一个满射。

对于任意 $x_1,x_2\in M$ 和 $y\in E$,如果 $s_1,s_2\in S$,使得 $f(s_1,y)=f(s_2,y)$,即 $e_{y}(s_1)=e_{y}(s_2)$,因为 e_y 是一个双射,于是 $s_1=s_2$,所以 $(S,E,M;f)$ 是一个认证码。

定理 2 以上构作 I 得到一个认证码,其参数分别为

$$|S|=l,|E|=|M|=n.$$

假定 $l\geq t$,那么成功地模仿攻击概率和成功地替换攻击概率分别为

$$P_1=\frac{(t+1)l}{n},P_s=\frac{l-1}{(t+1)l}.$$

证明:

根据 $\Gamma=(X,R)$ 的定义,有 $|S|=l,|E|=|M|=n$,则成功地模仿攻击概率为

$$P_1=\frac{k_1}{n},$$

即

$$P_1=\frac{(t+1)l}{n}.$$

成功地替换攻击概率为

$$P_s=\frac{\max_{1\leq j\leq d}P_{11}^j}{k_1}.$$

如果 $3\leq j\leq d$,那么 $P_{11}^j=0$,又因为 $P_{11}^1=a_1=l-1,P_{11}^2=c_2\leq t-1$,于是

$$P_s=\frac{P_{11}^1}{k_1}=\frac{l-1}{(t+1)l}.$$

3 对极距离正则图相关联的认证码

此处,总假定 $\Gamma=(X,R)$ 是 n 个点的直径为 d 的对极距离正则图。

构造 II 设信源集 S 是 Γ 中的 k_d 个点,设 $E=M=X$,对每一个点 $x \in X$,设 e_x 是一个从 S 到 $\Gamma_d(x)$ 的双射,对任意一个信源 s 和一个编码规则 x ,定义 $f(s,x)=e_x(s)$,那么 $(S,E,M;f)$ 是一个认证码。

定理 3 构造 II 是一个认证码。

证明:

根据以上的构造可知 $f(s,x)=e_x(s)$, $s \in S, x \in E$ 是一个映射。

对任意 $y \in M$,取 $x \in E$,得到一个双射 $e_x: S \rightarrow \Gamma_d(x)$,那么存在 $s \in S$,使得 $e_x(s)=x$,所以 f 是一个满射。

对于任意 $x_1, x_2 \in M$ 和 $y \in E$,如果 $s_1, s_2 \in S$,使得 $f(s_1, y)=f(s_2, y)$,即 $e_y(s_1)=e_y(s_2)$,这里 $s_1, s_2 \in S$,因为 e_y 是一个双射,所以 $s_1=s_2$,于是 $(S,E,M;f)$ 是一个认证码。

定理 4 以上构造 II 得到一个认证码,其参数分别为 $|S|=k_d, |E|=|M|=n$ 。成功地模仿攻击概率和成功地替换攻击概率分别为

$$P_1 = \frac{k_d}{n}, P_s = \frac{k_d - 1}{k_d}.$$

证明:

根据 $\Gamma=(X,R)$ 的定义可知 $|S|=k_d, |E|=|M|=n$ 。成功地模仿攻击概率为

$$P_1 = \frac{k_d}{n}.$$

成功地替换攻击概率为

$$P_s = \frac{\max_{1 \leq j \leq d} P_{dd}^j}{k_d},$$

如果 $1 \leq j \leq d-1$,那么 $P_{11}^j=0$,若 $j=d$,那么 $P_{dd}^d=k_d-1$,于是

$$P_s = \frac{P_{dd}^d}{k_d} = \frac{k_d - 1}{k_d}.$$

在此利用距离正则图的子图构造了 2 类较优的认证码,丰富和发展了距离正则图的应用。

参考文献:

- [1] WAN Z. Further construction of cartesian authentication codes from symplectic geometry[J]. Northeastern Mathematical Journal, 1992, 8: 4-20.
- [2] GAO S, GAO Y. Using a class of 1-dimensional non-isotropic subspaces in pseudo-symplectic geometry over a finite field to construct PBIB designs[J]. Northeastern Mathematical Journal, 1996, 2: 34-42.
- [3] WAN Z. Construction of cartesian authentication codes from unitary geometry[J]. Designs, Codes and Cryptology, 1992, 2: 333-356.
- [4] YOU H, GAO Y. Some new construction of Cartesian authentication codes from symplectic geometry[J]. System Sciences and Mathematical Sciences, 1994, 4: 317-327.
- [5] 高锁刚. 利用有限域上酉几何构造两类 Cartesian 认证码[J]. 高校应用数学学报 A 辑(中文版)(Applied Mathematic-A Journal), 1996, 11(3): 343-345.
- [6] BROUWER A E, COHEN A M, NEUMAIER A. Distance-Regular Graphs[M]. Berlin: Springer Verlag, 1989.

(上接第 10 页)

- [18] PARLOW J J, KURUMBAIL R G, STEGEMAN R A, et al. Design, synthesis, and crystal structure of selective 2-pyridone tissue factor VIIa inhibitors [J]. J Med Chem, 2003, 46: 4 696-4 701.
- [19] CARLES L, NARKUNAN K, PENLOU S, et al. 2-Pyridones from cyanoacetamides and enecarbonyl compounds: Application to the synthesis of nothapodytine B [J]. J Org Chem, 2002, 66: 4 304-4 308.
- [20] ZHUANG Qi-ya, JIA Run-hong, TU Shu-jiang, et al. Green chemistry approach to the synthesis of 2-amino-4-aryl-6-ferrocenyl-pyridine derivatives by a one-pot reaction in aqueous medium[J]. J Heterocyclic Chem, 2007, 44: 895-900.
- [21] JIA Run-hong, TU Shu-jiang. 2-Amino-4-(4-bromophenyl)-6-ferrocenylpyridine-3-Carbonitrile [J]. Acta Cryst, 2008, E64, m135.