Advances in Applied Mathematics 应用数学进展, 2021, 10(2), 544-547
Published Online February 2021 in Hans. http://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2021.102059

Hans汉斯

Galois环GR(2^2, 2^{2s})上的一类几乎差族

李丽彦，亓万锋，裴孟莹

辽宁师范大学数学学院，辽宁 大连
Email: qiwf@lnnu.edu.cn

收稿日期：2021年1月23日；录用日期：2021年2月17日；发布日期：2021年2月25日

摘　要

几乎差族在编码、通信安全等领域有着广泛的应用。本文利用Galois环GR(2^2, 2^{2s})上一种不相交的差族，通过对差族中某个集合添加一个元素，当满足一定条件时，即可构造出GR(2^2, 2^{2s})上的几乎差族。

关键词

Galois环，差族，几乎差族

A Family of Almost Difference Family on Galois Ring GR(2^2, 2^{2s})

Liyan Li, Wanfeng Qi, Mengying Pei

School of Mathematics, Liaoning Normal University, Dalian Liaoning
Email: qiwf@lnnu.edu.cn

Received: Jan. 23rd, 2021; accepted: Feb. 17th, 2021; published: Feb. 25th, 2021

Abstract

The almost difference family has a wide range of applications in coding, communication security and other fields. This paper uses one family of disjoint difference family on Galois ring GR(2^2, 2^{2s}), and by adding an element to a set in the difference family, when certain conditions are met, a new family of almost difference family can be constructed.

Keywords

Galois Ring, Difference Family, Almost Difference Family

文章引用: 李丽彦, 亓万锋, 裴孟莹. Galois 环 GR(2^2, 2^{2s})上的一类几乎差族[J]. 应用数学进展, 2021, 10(2): 544-547.
DOI: 10.12677/aam.2021.102059

1. 引言

随着对数论中环、域的深入了解，越来越多的学者对 Galois 环进行探究，Wan [1]曾在 *Lectures On Finite Fields And Galois Rings* 一书中详细地叙述了其基本理论内容。Galois 环不仅具有理论意义，在雷达、数字通信等领域也得到广泛应用。2014 年，李锦[2]发现可通过 Galois 环 $\mathrm{GR}\left(p^2,r\right)$ 的加法特征及乘法特征分别构造出高斯和与雅可比和并将其应用到通信中发展。与此同时也有学者着手在 Galois 环基础上探究各种差集、差族[3] [4]的构造方式，如 D. K. Ray-Chaudhuri [5]利用 $\mathrm{Z}_4\times\mathrm{Z}_4$ 同构于 $\mathrm{GR}\left(2^2,2\right)$ 构造出 $\mathrm{Z}_4\times\mathrm{Z}_4\times\mathrm{Z}_6$ 的差集。也有学者提出 Galois 环上 skew Hadamard 差集、差族[6] [7] [8] [9]构造方式并加以证明。本文从以往研究基础出发，对如何构造 $\mathrm{GR}\left(2^2,2^{2s}\right)$ 上几乎差族进行论述和研究，通过对差族中某个集合添加一个元素，当满足一定条件时，即可构造出 $\mathrm{GR}\left(2^2,2^{2s}\right)$ 上的几乎差族。

2. 基础知识

2.1. Galois 环相关知识

当 p 为素数，整数环 $Z_{p^2}=\left\{0,1,2,\cdots,p^2-1\right\}$，$g(x)$ 为 $Z_{p^2}[x]$ 中 s 次基本本原多项式，则称 $R=\mathrm{GR}\left(p^2,p^{2s}\right)=Z_{p^2}[x]/\left(g(x)\right)$ 是特征为 p^2，指数为 s 的 Galois 环，且存在 $g(x)$ 在环 R 中的根 ξ，阶数为 p^s-1。其中 R 中元素可表达成 $a_0+a_1x^1+a_2x^2+\cdots+a_{s-1}x^{s-1}+\left(g(x)\right),\left(a_i\in Z_{p^2}\right)$ 的形式，若 $\overline{g(x)}=g(x)(\mathrm{mod}\,p)$，则 $\overline{g(x)}$ 是 $F_p[x]$ 中本原多项式。易得到 mod p 映射：
$R=Z_{p^2}[x]/\left(g(x)\right)\xrightarrow{\text{“}-\text{”}}\overline{R}=F_p[x]/\overline{g(x)}=F_p^s$ 为环满同态。

环 R 中存在 $R\to Z_{p^2}$ 的迹映射 Tr，$\mathrm{Tr}(\alpha)=\sum_{i=0}^{s-1}\sigma^i(\alpha),(\alpha\in R)$，其中 $\sigma\left(\alpha_0+p\alpha_1\right)=\alpha_0^p+p\alpha_1^p\left(\alpha_0,\alpha_1\in T_{p^s}\right)$，以 $\overline{\mathrm{Tr}}:\overline{R}=F_p^s\to\overline{Z_{p^2}}=F_p$ 表示有限域的迹映射。

Galois 环 $\mathrm{GR}\left(p^2,p^{2s}\right)$ 中存在 Teichmuller 空间 $T_{p^s}^*=\langle\xi\rangle=\left\{1,\xi,\xi^2,\cdots,\xi^{p^s-2}\right\}$，$T_{p^s}=T_{p^s}^*\cup\{0\}$，$I_{p^s}=pT_{p^s}$，环 R 中元素也表达成 $\alpha=\alpha_0+p\alpha_1\left(\alpha_0,\alpha_1\in T_{p^s}\right)$。当 $p=2$ 时，$T_p^*=\{1\},T_p=\{0,1\}$。

R 中元素可分两部分，一部分为由素数 p 生成的主理想(p)，记为环 R 的唯一极大理想 M，$M=(p)=pR=\left\{py:y\in T_{p^s}\right\}=I_{p^s}$，另一部分为单位群 $\mathrm{GR}\left(p^2,p^{2s}\right)^*=R\setminus M=\left\{a+pb:a\in T_{p^s}^*,b\in T_{p^s}\right\}$。

2.2. 差族与几乎差族概念

定义[4] 设 G 为 v 阶加法交换群，$D_i\subset G$，且 $\left|D_i\right|=k_i\ (1\le i\le m)$，多重集 $\Delta D_i=\left\{a-b:a,b\in D_i,\text{且}a\ne b\right\}$。$D=\left\{D_1,D_2,\cdots,D_m\right\}$ 是一个集族，$\Delta D=\bigcup_{i=1}^m\Delta D_i=\bigcup_{i=1}^m\left\{a-b:a,b\in D_i,\text{且}a\ne b\right\}$，若 G 中有 t 个非零元素，每个元素都在 ΔD 中重复出现了 λ 次，剩余 $v-t-1$ 个非零元素中，每个元素在 ΔD 中重复出现 $\lambda+1$ 次，则称集族 $D=\left\{D_1,D_2,\cdots,D_m\right\}$ 是参数为 $\left\{v,\left\{k_1,k_2,\cdots,k_m\right\},\lambda,t\right\}$ 的几乎差族。当 $t=v-1$ 时 D 为差族。

3. 主要结果

据 Momihara Koji 在文献[7]中论述到，Galois 环 $\mathrm{GR}\left(2^2,2^{2s}\right)$ 中，$\overline{\mathrm{Tr}}$ 是 F_{2^s} 到 F_2 的迹映射，我们可以找到一组对应关系 g 从 F_{2^s}/F_2 映射到 $F_{2^s}^*$ 的差集，当 $\overline{\mathrm{Tr}}(\gamma)=1$ (其中 $\gamma\in F_{2^s}$)，可得到 $\left\{x:\overline{\mathrm{Tr}}(x)=1,x\in F_{2^s}^*\right\}=\left\{\beta^2+\beta+\gamma:\beta\in F_{2^s}\right\}$。$D=\left\{x^{-1}:\overline{\mathrm{Tr}}(x)=1,x\in F_{2^s}\right\}$ 为 $F_{2^s}^*$ 差集，双射 $g:F_{2^s}/F_2\to D$，$f=g^{-1}$，则有 $g\left(\beta+F_2\right)=\left(\beta^2+\beta+\gamma\right)^{-1}$。

下面定义两个映射σ_1,σ_2，根据 p 为 2 时 Galois 环$\mathrm{GR}\left(2^2,2^{2s}\right)$的元素性质可定义：$\sigma_1\left(\gamma^i\right)=\xi^i$，$\sigma_2\left(\gamma^i+F_2\right)=2\left(\xi^i+T_2\right)$，由此发现$\sigma_1:F_{2^s}^*\to T_{2^s}^*$，$\sigma_2:F_{2^s}/F_2\to I_{2^s}/I_2$，$f$为从$F_{2^s}^*$差集 D 到F_{2^s}/F_2的映射，若 X 为$T_{2^s}^*$差集，$Y=I_{2^s}/I_2$，可诱导出双射$h:X\to Y$. $P=p*T_2^*=\{2\}$。

引理 1 [7]. 若 h 为 X 到I_{2^s}/I_2的一组双射，$D_i=\xi^i\left(P\cup\left(\bigcup_{x\in X}x\left(1+h(x)\right)\right)\right)$，(其中$0\le i\le 2^s-2$)，$\left\{D_0,D_1,\cdots,D_{2^s-2}\right\}$是$\left(\mathrm{GR}\left(2^2,2^{2s}\right),+\right)$中参数为$\left\{2^{2s},\left\{2^s+1,2^s+1,\cdots,2^s+1\right\},2^s,2^{2s}-1\right\}$的差族。

定理 1. $\mathrm{GR}\left(2^2,2^{2s}\right)$中指数 s 为偶数时，令$D_i=\xi^i\left(P\cup\left(\bigcup_{x\in X}x\left(1+h(x)\right)\right)\right)$，(其中$0\le i\le 2^s-2$)，$\tilde{D}_0=D_0\cup\{a\}$，$\Delta\left(\tilde{D}_0\right)=\left\{x-y:x\in\tilde{D}_0,y\in\tilde{D}_0,x\ne y\right\}$。若不存在$x\in D_0$, $y\in D_0$满足方程$x+y=2a$，则$\left\{\tilde{D}_0,D_1,\cdots,D_{2^s-2}\right\}$是参数为$\left\{v,\left\{k_1,k_2,\cdots,k_m\right\},\lambda,t\right\}=\left\{2^{2s},\left\{2^s+2,2^s+1,\cdots,2^s+1\right\},2^s,2^{2s}-2^{s+1}-3\right\}$的$\mathrm{GR}\left(2^2,2^{2s}\right)$几乎差族，其中$\left\{2^s+2,2^s+1,\cdots,2^s+1\right\}$元素个数$m=2^s-1$。

证明 易知$\Delta\left(\tilde{D}_0\right)=\Delta\left(D_0\right)\cup\left(a-D_0\right)\cup\left(D_0-a\right)$。由假设知不存在$x\in D_0$, $y\in D_0$满足方程$a-x=y-a$，从而$\left(a-D_0\right)\cap\left(D_0-a\right)=\phi$。同时集合$a-D_0$中没有重复元素，集合$D_0-a$中亦没有重复元素，故$\left(a-D_0\right)\cup\left(D_0-a\right)$中元素仅出现一次。根据引理 1 知$\left\{D_0,D_1,\cdots,D_{2^s-2}\right\}$是$\mathrm{GR}\left(2^2,2^{2s}\right)$上参数为$\left\{2^{2s},\left\{2^s+1,2^s+1,\cdots,2^s+1\right\},2^s,2^{2s}-1\right\}$的差族。从而$\left\{\tilde{D}_0,D_1,\cdots,D_{2^s-2}\right\}$是参数为$\left\{2^{2s},\left\{2^s+2,2^s+1,\cdots,2^s+1\right\},2^s,2^{2s}-2^{s+1}-3\right\}$的几乎差族。

例 1. 当$s=2,a=1$时，设环$R_1=\mathrm{GR}\left(2^2,2^4\right)=Z_4[x]/\left(g_1(x)\right)=Z_4[\xi]$，其中$g_1(x)=x^2+x+1$，$\xi$为$g_1(x)$在$R_1$中的根，$\xi^2=3+3\xi$，环$R_1$的单位群$R_1^*=T_{2^2}^*\times\left(1+2T_{2^2}\right)$，其中$T_{2^2}^*=\left\{1,\xi,\xi^2\right\}$，$T_{2^2}=T_{2^2}^*\cup\{0\}$，$P=\{2\}$，构造$D_i=\xi^i\left(P\cup\left(\bigcup_{x\in X}x\left(1+h(x)\right)\right)\right)$，(其中$0\le i\le 2^s-2$)，$\tilde{D}_0=D_0\cup\{1\}$结果(见表 1)：

Table 1. Elements of almost difference familyon R_1
表 1. R_1中几乎差族元素

i	$D_i=\xi^i\left(P\cup\left(\bigcup_{x\in X}x\left(1+h(x)\right)\right)\right),\tilde{D}_0=D_0\cup\{1\}$
0	$\tilde{D}_0=\left\{1,2,3\xi^2,5\xi^2,\xi\left(1+2\xi\right),\xi\left(3+2\xi\right)\right\}$
1	$D_1=\left\{2\xi,3\xi^3,5\xi^3,\xi^2\left(1+2\xi\right),\xi^2\left(3+2\xi\right)\right\}$
2	$D_2=\left\{2\xi^2,3\xi^4,5\xi^4,\xi^3\left(1+2\xi\right),\xi^3\left(3+2\xi\right)\right\}$

计算$\left(\tilde{D}_0-\tilde{D}_0\right)\cup\left(D_1-D_1\right)\cup\left(D_2-D_2\right)$结果，将元素及其出现次数用有序数对表示如下：{0, 16}, {3, 5}, {3ξ, 5}, {2 + ξ, 5}, {3 + ξ, 5}, {3 + 3ξ, 5}, {1, 5}, {1 + 3ξ, 5}, {ξ, 5}, {2 + 2ξ, 4}, {3 + 2ξ, 4}, {2 + 3ξ, 5}, {1 + 2ξ, 4}, {2ξ, 4}, {1 + ξ, 5}, {2, 4}。将数对中元素重复出现的次数进行计数为：{16, 1}, {5, 10}, {4, 5}。

可以发现在$\mathrm{GR}\left(2^2,2^4\right)$中 5 个非零元素重复出现 4 次，10 个非零元素重复出现了 5 次，则$\left\{\tilde{D}_0,D_1,D_2\right\}$可构成 Galois 环上参数为$\left\{16,\left\{6,5,5\right\},4,5\right\}$的几乎差族。

例 2. 当$s=4,a=1$时，设环$R_2=\mathrm{GR}\left(2^2,2^8\right)=Z_4[x]/\left(g_2(x)\right)=Z_4[\xi]$，其中$g_2(x)=x^4+2x^2+3x+1$，环$R_2$的单位群$R_2^*=T_{2^4}^*\times\left(1+2T_{2^4}\right)$，其中$T_{2^4}^*=\left\{1,\xi,\xi^2,\xi^3,\xi^4,\xi^5,\xi^6,\xi^7,\xi^8,\xi^9,\xi^{10},\xi^{11},\xi^{12},\xi^{13},\xi^{14}\right\}$，$T_{2^4}=T_{2^4}^*\cup\{0\}$，$P=\{2\}$。构造$D_i=\xi^i\left(P\cup\left(\bigcup_{x\in X}x\left(1+h(x)\right)\right)\right)$，(其中$0\le i\le 2^s-2$)，$\tilde{D}_0=D_0\cup\{1\}$，部分结果如下：

$$\tilde{D}_0=\left\{1,2,3\xi^{12},5\xi^{12},\xi^4\left(1+2\xi\right),\xi^4\left(3+2\xi\right),\xi^3\left(1+2\xi^2\right),\xi^3\left(3+2\xi^2\right),\xi^9\left(1+2\xi^3\right),\xi^9\left(3+2\xi^3\right),\xi\left(1+2\xi^5\right),\right.$$
$$\left.\xi\left(3+2\xi^5\right),\xi^8\left(1+2\xi^6\right),\xi^8\left(3+2\xi^6\right),\xi^6\left(1+2\xi^7\right),\xi^6\left(3+2\xi^7\right),\xi^2\left(1+2\xi^{11}\right),\xi^2\left(3+2\xi^{11}\right)\right\},$$

$$D_1=\left\{2\xi,3\xi^{13},5\xi^{13},\xi^5\left(1+2\xi\right),\xi^5\left(3+2\xi\right),\xi^4\left(1+2\xi^2\right),\xi^4\left(3+2\xi^2\right),\xi^{10}\left(1+2\xi^3\right),\xi^{10}\left(3+2\xi^3\right),\xi^2\left(1+2\xi^5\right),\right.$$
$$\left.\xi^2\left(3+2\xi^5\right),\xi^9\left(1+2\xi^6\right),\xi^9\left(3+2\xi^6\right),\xi^7\left(1+2\xi^7\right),\xi^7\left(3+2\xi^7\right),\xi^3\left(1+2\xi^{11}\right),\xi^3\left(3+2\xi^{11}\right)\right\},$$

$$\vdots$$

$$D_{14}=\left\{2\xi^{14},3\xi^{26},5\xi^{26},\xi^{18}\left(1+2\xi\right),\xi^{18}\left(3+2\xi\right),\xi^{17}\left(1+2\xi^2\right),\xi^{17}\left(3+2\xi^2\right),\xi^{23}\left(1+2\xi^3\right),\right.$$
$$\xi^{23}\left(3+2\xi^3\right),\xi^{15}\left(1+2\xi^5\right),\xi^{15}\left(3+2\xi^5\right),\xi^{22}\left(1+2\xi^6\right),\xi^{22}\left(3+2\xi^6\right),\xi^{20}\left(1+2\xi^7\right),$$
$$\left.\xi^{20}\left(3+2\xi^7\right),\xi^{16}\left(1+2\xi^{11}\right),\xi^{16}\left(3+2\xi^{11}\right)\right\}.$$

计算$\left(\tilde{D}_0-\tilde{D}_0\right)\cup\left(\bigcup_{i=1}^{14}\left(D_i-D_i\right)\right)$结果可得到元素及其出现的次数，从中挑选出现相同次数的元素个数，记为有序数对：$\{256,1\},\{17,34\},\{16,221\}$，可以发现在$\mathrm{GR}\left(2^2,2^8\right)$中有 221 个非零元素重复出现 16 次，34 个非零元素重复 17 次，构成参数为$\left\{256,\{18,17,17,17,17,17,17,17,17,17,17,17,17,17,17\},16,221\right\}$的几乎差族。

经数值实验，当参数 s 取 6, 8, 10 等偶数时，仍然正确。我们给出如下猜测：

当 $\mathrm{GR}\left(2^2,2^{2s}\right)$ 中指数 s 为偶数时，令 $D_i=\xi^i\left(P\cup\left(\bigcup_{x\in X}x\left(1+h\left(x\right)\right)\right)\right)$，（其中 $0\le i\le 2^s-2$），$\tilde{D}_0=D_0\cup\{1\}$，则$\left\{\tilde{D}_0,D_1,\cdots,D_{2^s-2}\right\}$是$\mathrm{GR}\left(2^2,2^{2s}\right)$中参数为$\left\{2^{2s},\left\{2^s+2,2^s+1,\cdots,2^s+1\right\},2^s,2^{2s}-2^{s+1}-3\right\}$的几乎差族，其中$\left\{2^s+2,2^s+1,\cdots,2^s+1\right\}$元素个数共$2^s-1$个。

基金项目

辽宁省教育厅一般项目[LQ2020020]。

参考文献

[1] Wan, Z.X. (2003) Lectures on Finite Fields and Galois Rings. World Scientific Publishing Company, Singapore.

[2] 李锦. 伽罗华环上指数和及其在通信中的应用[D]: [博士学位论文]. 合肥: 合肥工业大学, 2014.

[3] 郑鹭亮, 林丽英. 基于 6 阶分圆数的广义几乎差集构造[J]. 龙岩学院学报, 2012, 30(5): 1-8.

[4] 刘永晴, 孔庆欣, 陆俞先, 汤静, 王天祎, 唐玲丽. 一些新的差族和几乎差族[J]. 应用数学进展, 2020, 9(3): 451-457.

[5] Ray-Chaudhuri, D.K. and Xiang, Q. (1996) Constructions of Partial Difference Sets and Relative Difference Sets Using Galois Rings. *Designs, Codes and Cryptography*, **8**, 215-227. https://doi.org/10.1007/BF00130580

[6] Momihara, K. (2012) Note on Divisible Difference Sets from Galois Rings GR (9, n). arXiv preprint arXiv:1210.1278

[7] Momihara, K. (2017) Disjoint Difference Families from Galois Rings. *The Electronic Journal of Combinatorics*, **24**, 3-23. https://doi.org/10.37236/6006

[8] Ding, C.S. and Yuan, J. (2005) A Family of Skew Hadamard Difference Sets. *Journal of Combinatorial Theory, Series A*, **113**, 1526-1535. https://doi.org/10.1016/j.jcta.2005.10.006

[9] Ding, C.S., Wang, Z.Y. and Xiang, Q. (2006) Skew Hadamard Difference Sets from the Ree-Tits Slice Symplectic Spreads in PG (3, 3^{2h+1}). *Journal of Combinatorial Theory, Series A*, **114**, 867-887.