Advances in Applied Mathematics 应用数学进展, 2022, 11(3), 1134-1139
Published Online March 2022 in Hans. http://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2022.113122

Hans汉斯

最优冲突回避码新的构造方法

黄必昌

百色学院，数学与统计学院，广西 百色

收稿日期：2022年2月21日；录用日期：2022年3月15日；发布日期：2022年3月22日

摘　要

目前，对最优冲突回避码的具体构造取得的结果不多，利用欧拉函数和同余数在整数环的特性给出一种构造的新方法，进一步具体构造码重k = 3，4，5，6时最优冲突回避码的一系列新结果。

关键词

冲突回避码，二次剩余，欧拉函数

New Constructions of Optimal Conflict-Avoiding Codes

Bichang Huang

College of Mathematics and Statistics, Baise University, Baise Guangxi

Received: Feb. 21st, 2022; accepted: Mar. 15th, 2022; published: Mar. 22nd, 2022

Abstract

Previously, there are very few results of explicit constructions of optimal conflict-avoiding code. In this paper, combing new constructions with Euler function and congruent numbers' properties in integer rings, a new infinite series of optimal conflict-avoiding codes with weight k = 3, 4, 5, 6 are obtained.

Keywords

Conflict-Avoiding Code, Quadratic Residue, Euler Function

文章引用: 黄必昌. 最优冲突回避码新的构造方法[J]. 应用数学进展, 2022, 11(3): 1134-1139.
DOI: 10.12677/aam.2022.113122

1. 引言

冲突回避码(Conflict-avoiding Code，简记 CAC)在无反馈多分址信道(冲突信道)有重要的应用[1] [2]。类似于文献[3]其数学描述如下：

设 $\mathbb{Z}_n$ 表示模 n 的剩余类环，$\mathbb{Z}_n^*$ 表示 $\mathbb{Z}_n \setminus \{0\}$。对于 k 阶子集 $A \subseteq \mathbb{Z}_n$，定义 A 的差集为多重集合

$$\Delta(A) = \{x - y \pmod n : x, y \in A, x \neq y\}.$$

设 $\mathcal{C}$ 是 $\mathbb{Z}_n$ 一些 k 阶子集 $A \subseteq \mathbb{Z}_n$ 的集合，则 $\mathcal{C}$ 被称为长度为 n 重量为 k 的冲突回避码若其满足以下条件

$$\Delta(A_1) \cap \Delta(A_2) = \varnothing, \ \forall A_1, A_2 \in \mathcal{C}, A_1 \neq A_2.$$

每个元素 $A \in \mathcal{C}$ 称为一个码字。对于给定的 n 和 k，符号 $\mathrm{CAC}(n,k)$ 表示所有长度为 n 重量为 k 的冲突回避码。

对于冲突回避码 $C \in \mathrm{CAC}(n,k)$，码字的重量 k (汉明码重量)表示用户在每个时段的 n 个时槽里发送 k 个数据包[4]。对于给定的正整数 n,k，如果 $C \in \mathrm{CAC}(n,k)$ 是一个码字个数最多的码，那么称 C 为一个最优码。

若 $A \subseteq Z_n$ 可以表示成为 $A = \{0, g, 2g, \cdots, (k-1)g\}, g \in Z_n^*$ 的形式，则称 A 为等差(equi-difference)码字。g 称为 A 的生成元。不难验证 $\Delta(A) = \{\pm g, \pm 2g, \cdots, \pm(k-1)g\}$。若码 $C \in \mathrm{CAC}(n,k)$ 的每个码字 $A \in C$ 都是等差码字，则称为 C 等差码。类似的，符号 $\mathrm{CAC}^{\mathrm{e}}(n,k)$ 表示所有长度为 n 重量为 k 的等差码。用符号 $\Gamma(C)$ 表示等差码 C 所有码字生成元的集合。等差码是一种特殊的码，人们通常利用它构造最优码。

目前，当 $k=3$ 时的最优冲突回避码构造证明已经基本解决[5]-[10]。当 $k>3$ 的最优冲突回避码具体构造较少[3] [4] [11]。本文利用利用欧拉函数和同余数在整数环的特性给出一种构造得新方法，给出新的构造方法，进一步给出当 $k=3,4,5,6$ 时对最优冲突回避码具体构造的一些新结果。

2. 相关的构造

为了方便理解，我们介绍一些常用的概念和符号。

设 $p = 2em+1$ 是奇素数，$\theta \in Z_p^*$ 是 Z_p^* 的生成元，设 $\theta \in H_0^{2e} = \{\theta^{2es} : s = 0,1,\cdots,m-1\}$ 是 Z_p^* 的 m 阶乘法子群，则 Z_p^* 有陪集分解：$Z_p^* = \bigcup_{i=0}^{2e-1} H_i^{2e}$，其中 $H_i^{2e} = \theta^i H_0^{2e}, 0 \le i \le 2e-1$ 称陪集 H_i^{2e} 为 $2e$ 阶分圆类。若 $j_t \in H_i^{2e}, 0 \le i \le 2e-1$。则称 $\{j_0, j_1, \cdots, j_{2e-1}\}$ 一个为 $2e$ 阶分圆类代表系。

引理 1 [4]. 设 $e \ge 1$ 和 $s > 1$ 都是整数，$p = 2em+1$ 是素数且使得每一个 $(\pm s, \pm 2s, \cdots, \pm es)$ 和 $(i-es, i-(e-1)s, \cdots, i+(e-1)s), 1 \le i \le s-1$ 都各自形成一个 $2e$ 阶分圆类代表系。那么存在一个码 $C \in \mathrm{CAC}^{\mathrm{e}}(sp, k = es+1)$ 包含 m 个码字，且满足 $Z_{sp} \setminus \Delta(C) = pZ_{sp}$。

引理 2 [11]. 若 $m > s$，则引理 1 构造的码 $C \in \mathrm{CAC}^{\mathrm{e}}(sp, k = es+1)$ 是最优的。

引理 3 [4]. 设 $k \ge 3$，L_1, L_2 和 s 都是正整数，且 $s \mid L_1$，$\gcd(l, L_2) = 1, l = 2,3,\cdots,(k-1)$。设 $C_1 \in \mathrm{CAC}^{\mathrm{e}}(L_1, k)$ 包含 m_1 个码字 $A_1, A_2, \cdots, A_{m_1}$ 使得

$$Z_{L_1}\setminus\bigcup_{j=1}^{m_1}\Delta(A_j)\supseteq\left(\frac{L_1}{s}\right)Z_{L_1}.$$

设 $C_2\in \mathrm{CAC}^{\mathrm{e}}(sL_2,k)$ 包含 m_2 个码字。设码 C 是由

$$\Gamma(C)=\left\{i+jL_1:i\in\Gamma(C_1),\ j\in Z_{L_1}\cup\left\{\left(\frac{L_1}{s}\right)y:y\in\Gamma(C_2)\right\}\right\}$$

生成。则 $C\in\mathrm{CAC}^{\mathrm{e}}(L_1L_2,k)$ 且包含 $m_1L_1+m_2$ 个码字。

利用引理 1 和引理 2 来具体构造一些最优冲突回避码。再利用引理 3 构造出一系列的冲突回避码 $C\in\mathrm{CAC}^{\mathrm{e}}\left((k-1)\prod_{i=1}^{r}p_i,k\right)$ [3] [4]。但是，实际情况下，我们很难得到最优 $C\in\mathrm{CAC}^{\mathrm{e}}\left((k-1)\prod_{i=1}^{r}p_i,k\right)$。本文首次利用欧拉函数和同余数的特性，对 $Z_{p^r}^*$ 进行划分，得到类似于引理 2 的一般构造，并给出具体构造码重 $k=3,4,5,6$ 时最优冲突回避码的一系列新结果。

3. 新的构造方法及其证明

设 n 为一个正整数，称 $G=\{a|(a,n)=1,a\in Z_n^*\}$ 是 Z_n^* 简约剩余系，则 $|G|=\Phi(n)$，其中 $\Phi(n)$ 是欧拉函数。显然，$G=\{a|(a,n)=1,a\in Z_n^*\}$ 是一个乘法群。

设 $p=2m+1$ 是奇素数，r 为一个正整数，元素 $\theta_j\in Z_{p^j}^*$ 是乘法群 $G_j=\{a|(a,n)=1,a\in Z_{p^j}^*\},1\le j\le r.$ 的一个生成元，则 $|G_j|=\Phi(p^j)$。又设 $H_{j0}^2=\{\theta^{2s}:s=0,1,\cdots,m-1\},1\le j\le r$ 是 $G_j=\{a|(a,n)=1,a\in Z_{p^j}^*\}$ 的 m 阶乘法子群，则 G_j 有陪集分解：$G_j=H_{j0}^2\cup H_{j1}^2$，其中 $H_{j1}^2=\theta_j^1H_{j0}^2$，称陪集 H_{ji}^2 为 2 阶分圆类。若 $d_i\in H_{ji}^2,0\le i\le 1$。则称 $\{d_0,d_1\}$ 为 G_j 的一个 2 阶分圆类代表系。下面得到类似于引理 2 的一般构造。

定理 1. 设 s,r 是正整数，p 是奇素数且使得每一个 $(i-s,i),1\le i\le s-1$ 和 $(\pm s)$ 都各自形成 $G_j,\ j=1,2,\cdots,r$ 的一个 2 阶分圆类代表系。那么存在一个码 $C\in\mathrm{CAC}^{\mathrm{e}}(sp^r,k=s+1)$ 包含 $\frac{p^r-1}{2}$ 个码字，且满足 $Z_{sp^r}\setminus\Delta(C)=pZ_{sp^r}$。

证 在 $Z_s\times Z_{p^r}$ 上设 $\Gamma_j(C)=\{1\}\times(p^{r-j}H_{jo}^2),\ j=1,2,\cdots,r.$ 则 C 的码字表示如下：

$$x_j^l=\{(0,0),(1,1),\cdots,((k-1),(k-1))\}\cdot\{1,p^{r-j}\theta_j^{2l}\},l=0,1,\cdots,\Phi(p^j),\ j=1,2,\cdots,r.$$

故

$$\Delta(x_j^l)=\begin{cases}\{0\}\times\{s\theta_j^2p^{r-j},-s\theta_j^2p^{r-j}\}, & i=0,\\ \{i\}\times\{(i-s)\theta_j^2p^{r-j},i\theta_j^2p^{r-j}\},1\le i\le s-1,\end{cases}$$

即

$$\begin{aligned}\Delta(C)&=\bigcup_{j=1}^{r}\bigcup_{l=1}^{\Phi(p^j)}\Delta(x_j^l)\\&=\bigcup_{j=1}^{r}\left(\bigcup_{i=1}^{s-1}(\{i\}\times(p^{r-j}H_{jo}^2))\cdot(i-s,i)\right)\cup\left((\{0\}\times(p^{r-j}H_{jo}^2))\cdot(-s,s)\right)\\&=\bigcup_{j=1}^{r}\bigcup_{i=1}^{s-1}(\{i\}\times(p^{r-j}G_j))\\&=Z_s\times Z_{p^r}^*\end{aligned}$$

由 $s=k-1$， $p^r-1=\sum_{j=1}^{r}\Phi\left(p^j\right)$ 得， $|C|=\frac{s\sum_{j=1}^{r}\Phi\left(p^j\right)}{2(k-1)}=\frac{s\left(p^r-1\right)}{2(k-1)}=\frac{p^r-1}{2}$。

定理 2. 定理 1 构造的码 $C\in \mathrm{CAC}^{\mathrm{e}}\left(sp^r,k=s+1\right)$ 是最优的。

因为 $\left\lfloor\frac{sp^r-1}{2(k-1)}\right\rfloor=\left\lfloor\frac{sp^r-s+s-1}{2(k-1)}\right\rfloor=\left\lfloor\frac{sp^r-s+s-1}{2s}\right\rfloor=\frac{p^r-1}{2}$。

下面，根据同余性质结合定理 1 具体构造码重 $k=3,4,5,6$ 时最优冲突回避码的一系列新结果，由定理 2 知，结果是最优的。

设 p 是奇素数，对于 $a\in Z_p^*$，若同余方程 $x^2\equiv a\pmod p$ 有解，称 a 为模 p 的二次剩余(quadratic residue) (即 $a\in H_0^2$)。否则，称 a 模 p 的二次非剩余(quadratic non-residue) $a\in H_1^2$。定义 Z_p 上的勒让德符号 $\left(\frac{a}{p}\right)$ 为：

$$\left(\frac{a}{p}\right)=\begin{cases}1, & \text{若} a\in H_0^2,\\ -1, & \text{若} a\in H_1^2,\\ 0, & \text{若} p\mid a.\end{cases}$$

且具有性质 $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$。

关于勒让德符号有如下结果。

引理 4 [12]. 若 p 是奇素数，则

$$\left(\frac{-1}{p}\right)=\begin{cases}1, & \text{若} p\equiv 1\pmod 4,\\ -1, & \text{若} p\equiv 3\pmod 4.\end{cases}$$

$$\left(\frac{2}{p}\right)=\begin{cases}1, & \text{若} p\equiv \pm 1\pmod 8,\\ -1, & \text{若} p\equiv \pm 3\pmod 8.\end{cases}$$

$$\left(\frac{3}{p}\right)=\begin{cases}1, & \text{若} p\equiv \pm 1\pmod{12},\\ -1, & \text{若} p\equiv \pm 5\pmod{12}.\end{cases}$$

引理 5 [13]. 同余方程 $x^2\equiv a\pmod{p^j}$, $j=1,2,3,\cdots,r$，有解的充要条件是 $\left(\frac{a}{p}\right)=1$。

推论 1. 若素数 $p\equiv 7\pmod 8$， r 是正整数，则存在最优码 $C\in \mathrm{CAC}^{\mathrm{e}}\left(2p^r,3\right)$ 包含 $\frac{p^r-1}{2}$ 个码字。

证 根据定理 1~2 和引理 4~5 并结合勒让德符号的性质，在 G_j, $j=1,2,\cdots,r$ 中只需证 $\left(\frac{a}{p}\right)\neq\left(\frac{b}{p}\right)$ 对于每对 $\{a,b\}\in\{\{-2,2\},\{-1,2\}\}$。即只需证

$$\left(\frac{-1}{p}\right)=-1,\ \left(\frac{2}{p}\right)=1.$$

而当 $p\equiv 7\pmod 8$ 时以上条件满足。从而命题得证。

推论 2. 若素数 $p\equiv 7\pmod 8$， r 是正整数，则存在最优码 $C\in \mathrm{CAC}^{\mathrm{e}}\left(3p^r,4\right)$ 包含 $\frac{p^r-1}{2}$ 个码字。

证 根据定理 1~2 和引理 4~5 并结合勒让德符号的性质，在 $G_j, j=1,2,\cdots,r$ 中只需证 $\left(\frac{a}{p}\right)\neq\left(\frac{b}{p}\right)$ 对于每对 $\{a,b\}\in\{\{-3,3\}\{-2,1\},\{-1,2\}\}$。即只需证

$$\left(\frac{-1}{p}\right)=-1,\ \left(\frac{2}{p}\right)=1.$$

而当 $p\equiv 7\pmod 8$ 时以上条件满足。从而命题得证。

推论 3. 若素数 $p\equiv 11\pmod{12}$，r 是正整数，则存在最优码 $C\in \mathrm{CAC}^{\mathrm{e}}\left(4p^r,5\right)$ 包含 $\frac{p^r-1}{2}$ 个码字。

证 根据定理 1~2 和引理 4~5 并结合勒让德符号的性质，在 $G_j, j=1,2,\cdots,r$ 中只需证 $\left(\frac{a}{p}\right)\neq\left(\frac{b}{p}\right)$ 对于每对 $\{a,b\}\in\{\{-4,4\},\{-3,1\},\{-2,2\},\{-1,3\}\}$。即只需证

$$\left(\frac{-1}{p}\right)=-1,\ \left(\frac{3}{p}\right)=1.$$

而当 $p\equiv 11\pmod{12}$ 时以上条件满足。从而命题得证。

推论 4. 若素数 $p\equiv 23\pmod{24}$，r 是正整数，则存在最优码 $C\in \mathrm{CAC}^{\mathrm{e}}\left(5p^r,6\right)$ 包含 $\frac{p^r-1}{2}$ 个码字。

证 根据定理 1~2 和引理 4~5 并结合勒让德符号的性质，在 $G_j, j=1,2,\cdots,r$ 中只需证 $\left(\frac{a}{p}\right)\neq\left(\frac{b}{p}\right)$ 对于每对 $\{a,b\}\in\{\{-5,5\},\{-4,1\},\{-3,2\},\{-2,1\},\{-1,4\}\}$。即只需证

$$\left(\frac{-1}{p}\right)=-1,\ \left(\frac{2}{p}\right)=\left(\frac{3}{p}\right)=1.$$

而当 $p\equiv 23\pmod{24}$ 时以上条件满足。从而命题得证。

4. 结论

本文给出新的构造方法具体构造出一系列最优的冲突回避码得。该方法也可以给光正交码的构造提供借鉴。

基金项目

广西自然科学基金项目(2018GXNSFAA281259)。

参考文献

[1] Massey, J.L. and Mathys, P. (1985) The Collision Channel without Feedback. *IEEE Transactions on Information Theory*, **31**, 192-204. https://doi.org/10.1109/TIT.1985.1057010

[2] Gryorfi, N.Q.A.L. and Massey, J.L. (1992) Constructions of Binary Constant Weight Cyclic Codes and Cyclically Permutable Codes. *IEEE Transactions on Information Theory*, **38**, 940-949. https://doi.org/10.1109/18.135636

[3] 黄必昌, 朱文兴. 最优冲突回避码的具体构造[J]. 福州大学学报(自然科学版), 2016, 44(3): 390-393.

[4] Momihara, K., Muller, M., Satoh, J., *et al.* (2008) Constant Weight Conflict-Avoiding Codes. *Siam Journal on Discrete Mathematics*, **21**, 959-979. https://doi.org/10.1137/06067852X

[5] Fu, H.L., Li, Y.H. and Mishima, M. (2011) Errata to "Optimal Conflict-Avoiding Codes of Even Length and Weight 3". *IEEE Transactions on Information Theory*, **57**, 5572-5572. https://doi.org/10.1109/TIT.2011.2107878

[6] Jimbo, M., Mishima, M., Janiszewski, S., *et al.* (2007) On Conflict-Avoiding Codes of Length n = 4 m for Three Ac-

tive Users. *IEEE Transactions on Information Theory*, **53**, 2732-2742. https://doi.org/10.1109/TIT.2007.901233

[7] Levenshtein, V.I. (2007) Conflict-Avoiding Codes and Cyclic Triple Systems. *Problems of Information Transmission*, **43**, 199-212. https://doi.org/10.1134/S0032946007030039

[8] Mishima, M., Fu, H.L. and Uruno, S. (2009) Optimal Conflict Avoiding Codes of Length n = (0 mod16) and Weight 3. *Designs, Codes and Cryptography*, **52**, 275-291. https://doi.org/10.1007/s10623-009-9282-2

[9] Momihara, K. (2007) Necessary and Sufficient Conditions for Tight Equi-Difference Conflict-Avoiding Codes of Weight Three. *Designs, Codes and Cryptography*, **45**, 379-390. https://doi.org/10.1007/s10623-007-9139-5

[10] Ma, W.P., Zhao, C.E. and Shen, D.S. (2014) New Optimal Constructions of Conflict-Avoiding Codes of Odd Length and Weight 3. *Designs, Codes and Cryptography*, **73**, 791-804. https://doi.org/10.1007/s10623-013-9827-2

[11] Shum, K.W., Wong, W.S. and Chen, C.S. (2010) A General Upper Bound on the Size of Constant Weight Conflict Avoiding Codes. *IEEE Transactions on Information Theory*, **56**, 3265-3276. https://doi.org/10.1109/TIT.2010.2048508

[12] Nathanson, M.B. (2000) Elementary Methods in Number Theory. Springer-Verlag, New York.

[13] 蔡天新. 数论: 从同余的观点出发[M]. 北京: 高等数学出版社, 2012.