

DOI: 10.20098/j.cnki.1001-5132.2023.0604

集合差系统的新构造

沈淑钰, 包经俊*

(宁波大学 数学与统计学院, 浙江 宁波 315211)

摘要: 研究集合差系统新的构造方法. 借助有限域上分圆类, 给出集合差系统的两个直接构造; 再利用克罗内克积建立集合差系统新的递归构造, 并推广了已知构造. 最后应用所得到的直接构造和递归构造给出了新的渐近最优的集合差系统.

关键词: 集合差系统; 分圆类; 差覆盖; 码字同步

中图分类号: O157.2

文献标志码: A

文章编号: 1001-5132 (2024) 02-0078-08

为解决码字同步问题, Levenshtein^[1]于 1971 年引入一个新组合结构, 称为集合差系统(Difference System of Sets, DSS).

设 $\mathcal{T} = \{A_0, A_1, \dots, A_{t-1}\}$ 是由 $\mathbb{Z}_n$ 上 t 个不相交子集(称为区组)组成的集族, $K = \{|A_i| : i = 0, 1, \dots, t-1\}$ 为区组大小的多重集. 定义 $\Delta_E(\mathcal{T})$ 为 $\mathcal{T}$ 中子集之间外差的多重集, 即

$$\Delta_E(\mathcal{T}) = \{a - b \pmod n : a \in A_i, b \in A_j, 0 \leq i \neq j \leq t-1\}. \quad (1)$$

若 $\Delta_E(\mathcal{T})$ 包含 $\mathbb{Z}_n$ 中每个非零元至少 ρ 次, 则称集族 $\mathcal{T}$ 为 (n, K, t, ρ) 集合差系统, 记为 (n, K, t, ρ) -DSS.

若 $\mathbb{Z}_n$ 中每个非零元在多重集(1)式中都恰好出现 ρ 次, 则称该 DSS 是完美的. 若所有区组的大小相同, 即 $|A_0| = |A_1| = |A_2| = \dots = |A_{t-1}| = m$, 称该 DSS 是正则的, 记为 (n, m, t, ρ) -DSS.

给定 $\mathbb{Z}_n$ 上的一个 (n, m, t, ρ) -DSS $\{A_0, A_1, \dots, A_{t-1}\}$, 其冗余 r 为各个区组大小的和, 即

$$r = \sum_{i=0}^{t-1} |A_i|.$$

设 $r = r_t(n, \rho)$ 为给定参数下最小的冗余, 若 DSS 的冗余 $r = r_t(n, \rho)$, 则称该 DSS 是最优的.

Levenshtein^[1]得到了 $r = r_t(n, \rho)$ 的一个下界, Wang^[2]则对此下界做了改进, 为

$$r_t(n, \rho) \geq \left\lceil \sqrt{\frac{t\rho(n-1)}{t-1}} \right\rceil,$$

其中, $\lceil x \rceil$ 表示大于等于 x 的最小整数.

设存在一类无限的 DSS, 若其参数为 (n, K, t, ρ) 和冗余 r 满足

$$\lim_{n \rightarrow +\infty} \frac{\sqrt{\frac{t\rho(n-1)}{t-1}}}{r} = 1, \quad (2)$$

则称此类 DSS 是渐近最优的^[3].

近年来, 国内外学者也对 DSS 的构造进行了许多研究. Tochev^[4-5]通过循环差集、分圆类与重量矩阵得到构造 DSS 新的方法. Fuji-Hara 等^[6]通过有限几何中的超平面划分方法构造了 DSS. 范翠玲等^[7-8]分别通过不相交差族和差集构造 DSS. Qi 等^[9]通过 12 阶的分圆类差集来得到新的 DSS. Fujiwara 等^[10]通过由两个阶数互素 DSS 所构造的乘积方法得到了新的 DSS. Wang 等^[11]通过差集和划分型 DSS 给出新的构造. Lei 等^[12-13]通过划分型的循环差填充以及有限射影几何构造 DSS. 王红瑞^[14]通过线性空间、子群陪集、结合方案构造出新的 DSS. Chisaki 等^[3]通过差覆盖和划分型的 DSS 得到 DSS 的递推构造. 还有学者利用代数、组合的方法构造了可划分差填充^[15-16], 并由此可构造 DSS. 这些构造都可得到许多最优与渐近最优 DSS.

收稿日期: 2023-06-12.

宁波大学学报(理工版)网址: <http://journalg.nbu.edu.cn/>

基金项目: 国家自然科学基金(11701303).

第一作者: 沈淑钰, 硕士研究生, 主要研究方向: 组合数学. E-mail: 1162659967@qq.com

*通信作者: 包经俊, 博士/副教授, 主要研究方向: 组合数学. E-mail: baojingjun@nbu.edu.cn

本文首先通过有限域上分圆类得到两类新的渐近最优 DSS 的直接构造, 再利用克罗内克积给出一个新的递归构造, 并将其应用于已知 DSS 中, 以得到新的渐近最优 DSS.

1 预备知识

设 $\mathcal{H} = \{B_0, B_1, \dots, B_{t-1}\}$ 是由 $\mathbb{Z}_v$ 上 t 个子集(称为区组)组成的集族, $K = \{i | B_i : 0 \leq i \leq t-1\}$ 为区组大小的多重集. 定义 $\Delta(\mathcal{H})$ 为 $\mathcal{H}$ 中子集内差的多重集, 即

$$\Delta(\mathcal{H}) = \{a - b \pmod{n} : a, b \in B_i, a \neq b, 0 \leq i \leq t-1\}.$$

若 $\Delta(\mathcal{H})$ 包含 $\mathbb{Z}_v$ 中的每个非零元至多 λ 次, 则称集族 $\mathcal{H}$ 为 $\mathbb{Z}_v$ 上 (v, K, λ) 循环差填充(Cyclic Difference Packing, CDP), 记为 t -CDP (v, K, λ) . 若 $\Delta(\mathcal{H})$ 包含 $\mathbb{Z}_v$ 中的每个非零元至少 λ 次, 则称集族 $\mathcal{H}$ 为 $\mathbb{Z}_v$ 上 (v, K, λ) 循环差覆盖(Cyclic Difference Covering, CDC), 记为 t -CDC (v, K, λ) . 若 $\Delta(\mathcal{H})$ 包含 $\mathbb{Z}_v$ 中的每个非零元恰好 λ 次, 则称集族 $\mathcal{H}$ 为 $\mathbb{Z}_v$ 上 (v, K, λ) 循环差族(Cyclic Difference Family, CDF), 记为 t -CDF (v, K, λ) . 若所有区组的大小皆为 k , 可记为 t -CDP (v, K, λ) (或者对应的 t -CDC (v, K, λ) 、 t -CDF (v, K, λ)). 当 $t=1$ 时, 记 1-CDC (v, K, λ) 为 CDC (v, K, λ) , 且记 1-CDF (v, K, λ) 为 DS (v, K, λ) .

设集族 $\mathcal{H} = \{B_0, B_1, \dots, B_{t-1}\}$ 为 $\mathbb{Z}_v$ 上区组不相交的 DSS 或 CDP. 若 $\bigcup_{i=0}^{t-1} B_i = \mathbb{Z}_v$ 或 $\bigcup_{i=0}^{t-1} B_i = L$ 且 L 是一个差覆盖, 则称 $\mathcal{H}$ 为 $\mathbb{Z}_v$ 或差覆盖 L 上的划分型设计.

为更简洁明了地介绍接下来的构造, 引入以下符号: 设 X, Y 是 $\mathbb{Z}_n$ 上给定的多重集, $\mathcal{H} = \{B_0, B_1, \dots, B_{t-1}\}$ 是 $\mathbb{Z}_n$ 上 t 个子集组成的集族, m 是正整数.

定义以下多重集:

$$\Delta_E(X, Y) = \{a - b \pmod{n} : a \in X, b \in Y\},$$

$$\Delta_E(\mathcal{H}) = \{a - b \pmod{n} : a \in B_i, b \in B_j, 0 \leq i \neq j < t\},$$

$$\Delta(Y) = \{a - b \pmod{n} : a, b \in Y, a \neq b\},$$

$$\Delta(\mathcal{H}) = \{a - b \pmod{n} : a, b \in B_i, a \neq b, 0 \leq i < t\},$$

$$[m] = \{1, 2, \dots, m\}, \quad m\mathbb{Z}_{mn} = \{0, m, \dots, (n-1)m\},$$

$X = \underline{m}Y$ 表示 Y 中的每个元素在 X 中恰好出现 m 次,

$X \geq \underline{m}Y$ 表示 Y 中的每个元素在 X 中至少出现 m 次,

$X \leq \underline{m}Y$ 表示 Y 中的每个元素在 X 中至多出现 m 次,

$X \cup Y$ 表示 X 与 Y 关于多重集的并.

2 集合差系统的直接构造

在构造集合差系统时, 有限域上分圆类起着重要作用. 此节将介绍利用分圆类得到几类渐近最优集合差系统的直接构造, 并做出所需的一些定义与结论.

设 p 是一个素数, e 是一个正整数且满足 $e | (p-1)$. 设 β 是有限域 $\mathbb{F}_p$ 上的一个本原元. 令 $\langle \beta^e \rangle$ 为乘法群 $\mathbb{F}_p \setminus \{0\}$ 中由 β^e 生成的子群, 定义分圆陪集 $C_i^{(e,p)} = \beta^i \langle \beta^e \rangle, i = 0, 1, \dots, e-1$. 陪集 $C_0^{(e,p)}, C_1^{(e,p)}, \dots, C_{e-1}^{(e,p)}$ 则称为 $\mathbb{F}_p$ 上 e 阶分圆类.

引理 1^[4] 设 $p = ef + 1$ 是一个素数, 则 $\{C_0^{(e,p)}, C_1^{(e,p)}, \dots, C_{e-1}^{(e,p)}\}$ 是一个完美且正则的 $(p, f, e, f(e-1))$ -DSS.

引理 2 若存在一个包含区组 $\{0\}$ 的划分型 t -CDP (v, K, λ) , 则存在一个 $(v, K \setminus \{1\}, t-1, v-\lambda-2)$ -DSS.

证明 设 $\{B_0 = \{0\}, B_1, \dots, B_{t-1}\}$ 是一个划分型 t -CDP (v, K, λ) ,

$$\text{则 } \bigcup_{i=0}^{t-1} B_i = \mathbb{Z}_v \text{ 且 } \bigcup_{i=0}^{t-1} \Delta(B_i) \leq \underline{\lambda}(\mathbb{Z}_v \setminus \{0\}).$$

由于 $\Delta_E(\mathbb{Z}_v, \mathbb{Z}_v) = \underline{v}\mathbb{Z}_v$, 则

$$\bigcup_{i=1}^{t-1} \bigcup_{j=1}^{t-1} \Delta_E(B_i, B_j) = \bigcup_{i=1}^{t-1} \Delta_E \left(B_i, \bigcup_{j=1}^{t-1} B_j \right) =$$

$$\bigcup_{i=1}^{t-1} \Delta_E(B_i, \mathbb{Z}_v \setminus (B_i \cup \{0\})) =$$

$$\bigcup_{i=1}^{t-1} \Delta_E(B_i, \mathbb{Z}_v) \setminus \bigcup_{i=1}^{t-1} \Delta_E(B_i, B_i \cup \{0\}) =$$

$$\underline{(v-2)}(\mathbb{Z}_v \setminus \{0\}) \setminus \bigcup_{i=0}^{t-1} \Delta(B_i) \geq$$

$$\underline{(v-\lambda-2)}(\mathbb{Z}_v \setminus \{0\}).$$

因此, $\{B_1, \dots, B_{t-1}\}$ 是一个 $(v, K \setminus \{1\}, t-1, v-\lambda-2)$ -DSS.

定理 1 设 $p = ef + 1$ 是一个素数, 其中 e 为奇数, 则存在一个 $(p, \{2f, \dots, 2f, f\}, (e+1)/2, p-3f-1)$ -DSS, 且冗余为 $r = ef$.

证明 设 $C_0^{(e,p)}, C_1^{(e,p)}, \dots, C_{e-1}^{(e,p)}$ 是 $\mathbb{Z}_p$ 上 e 阶的分圆类, 构造如下 $\mathbb{Z}_p$ 上的 $(e+1)/2$ 个子集:

$$A_0 = C_0^{(e,p)} \cup C_{\frac{e-1}{2}}^{(e,p)}, A_1 = C_1^{(e,p)} \cup C_{\frac{e-1}{2}}^{(e,p)}, \dots, \\ A_{\frac{e-3}{2}} = C_{\frac{e-3}{2}}^{(e,p)} \cup C_{e-2}^{(e,p)}, A_{\frac{e-1}{2}} = C_{e-1}^{(e,p)}.$$

由引理 1 可得, 集族 $\{C_0^{(e,p)}, C_1^{(e,p)}, \dots, C_{e-1}^{(e,p)}\}$ 是一个完美且正则的 $p, f, e, f(e-1)$ -DSS, 同时由

$$\bigcup_{i=0}^{e-1} C_i^{(e,p)} = \mathbb{Z}_p \setminus \{0\}$$

可得:

$$\bigcup_{i=0}^{e-1} \Delta(C_i^{(e,p)}) = \Delta\left(\bigcup_{i=0}^{e-1} C_i^{(e,p)}\right) \setminus \\ \bigcup_{0 \leq i \neq i' \leq e-1} \Delta_E(C_i^{(e,p)}, C_{i'}^{(e,p)}) = \\ (f-1)(\mathbb{Z}_p \setminus \{0\}).$$

设 $\mathcal{T} = \{A_0, A_1, \dots, A_{\frac{e-3}{2}}, A_{\frac{e-1}{2}}\}$, 则 $\mathcal{T}$ 是 $\mathbb{Z}_p \setminus \{0\}$ 的划分.

下面计算 $\Delta(\mathcal{T})$.

$$\Delta(\mathcal{T}) = \bigcup_{i=0}^{\frac{e-1}{2}} \Delta(A_i) = \\ \bigcup_{i=0}^{\frac{e-3}{2}} \Delta\left(C_i^{(e,p)} \cup C_{\frac{e-1}{2}}^{(e,p)}\right) \cup \Delta\left(C_{\frac{e-1}{2}}^{(e,p)}\right) = \\ \bigcup_{i=0}^{e-1} \Delta(C_i^{(e,p)}) \cup \bigcup_{i=0}^{\frac{e-3}{2}} \left(\Delta_E\left(C_i^{(e,p)}, C_{\frac{e-1}{2}}^{(e,p)}\right) \cup \right. \\ \left. \Delta_E\left(C_{\frac{e-1}{2}}^{(e,p)}, C_i^{(e,p)}\right)\right) = \\ (f-1)(\mathbb{Z}_p \setminus \{0\}) \cup \bigcup_{i=0}^{\frac{e-3}{2}} \left(\Delta_E\left(C_i^{(e,p)}, C_{\frac{e-1}{2}}^{(e,p)}\right) \cup \right. \\ \left. \Delta_E\left(C_{\frac{e-1}{2}}^{(e,p)}, C_i^{(e,p)}\right)\right). \quad (3)$$

直接计算可知, 有等式

$$\Delta_E\left(C_{\frac{e-1}{2}}^{(e,p)}, C_i^{(e,p)}\right) = C_i^{(e,p)} \left(C_{\frac{e-1}{2}}^{(e,p)} - 1\right),$$

$$\Delta_E\left(C_i^{(e,p)}, C_{\frac{e-1}{2}}^{(e,p)}\right) = C_i^{(e,p)} \left(1 - C_{\frac{e-1}{2}}^{(e,p)}\right).$$

又因为

$$\bigcup_{i=0}^{\frac{e-3}{2}} C_i^{(e,p)} \left(C_{\frac{e-1}{2}}^{(e,p)} - 1\right) \leq \underline{f}(\mathbb{Z}_p \setminus \{0\}),$$

$$\bigcup_{i=0}^{\frac{e-3}{2}} C_i^{(e,p)} \left(1 - C_{\frac{e-1}{2}}^{(e,p)}\right) \leq \underline{f}(\mathbb{Z}_p \setminus \{0\}),$$

代入(3)式可得

$$\Delta(\mathcal{T}) \leq (f-1)(\mathbb{Z}_p \setminus \{0\}) \cup 2f(\mathbb{Z}_p \setminus \{0\}) =$$

$$(3f-1)(\mathbb{Z}_p \setminus \{0\}).$$

再由引理 2 可得

$$\Delta_E(\mathcal{T}) \geq (p-2-(3f-1))(\mathbb{Z}_p \setminus \{0\}) = \\ (p-3f-1)(\mathbb{Z}_p \setminus \{0\}).$$

综上可得, $\mathcal{T}$ 是一个 $(p, \{2f, \dots, 2f, f\}, (e+1)/2, p-3f-1)$ -DSS, 且冗余为 $r = 2f(e+1)/2 + f = ef$.

推论 1 当 $e \rightarrow \infty$ 时, $(p, \{2f, \dots, 2f, f\}, (e+1)/2, p-3f-1)$ -DSS 是渐近最优的.

证明 由定理 1 中构造可知

$$\frac{t\rho(n-1)}{r^2(t-1)} = \frac{(e+1)(ef+1-3f-1)(ef+1-1)}{(ef)^2(e-1)} = \\ \frac{e+1}{e-1} \cdot \frac{f(e-3)}{ef} = \frac{e+1}{e-1} \cdot \left(1 - \frac{3}{e}\right).$$

显然当 $e \rightarrow \infty$ 时, 有

$$\lim_{e \rightarrow \infty} \frac{t\rho(n-1)}{r^2(t-1)} = 1,$$

即所得 DSS 是渐近最优的.

定理 2 设 $p = ef + 1$ 为一个素数, 其中 e 为奇数. 则存在一个 $(p, 2f, (e-1)/2, p-5f-1)$ -DSS, 且冗余为 $r = ef - f$.

证明 设集族 $\mathcal{T} = \{A_0, A_1, \dots, A_{\frac{e-3}{2}}, A_{\frac{e-1}{2}}\}$ 如定理 1 中的构造. 由定理 1 可知

$$\Delta_E(\mathcal{T}) \geq (p-3f-1)(\mathbb{Z}_p \setminus \{0\}).$$

取出子集 $A_0, A_1, \dots, A_{\frac{e-3}{2}}$, 构成集族 $\mathcal{T}' = \{A_0, A_1, \dots, A_{\frac{e-3}{2}}\}$.

下面计算 $\Delta_E(\mathcal{T}')$.

$$\Delta_E(\mathcal{T}') = \bigcup_{i=0}^{\frac{e-3}{2}} \bigcup_{\substack{j=0 \\ j \neq i}}^{\frac{e-3}{2}} \Delta_E(A_i, A_j) = \Delta_E(\mathcal{T}) \setminus \\ \left(\bigcup_{i=0}^{\frac{e-3}{2}} \Delta_E\left(A_i, A_{\frac{e-1}{2}}\right) \cup \bigcup_{i=0}^{\frac{e-3}{2}} \Delta_E\left(A_{\frac{e-1}{2}}, A_i\right) \right).$$

又由 $\bigcup_{i=0}^{\frac{e-3}{2}} A_i \cup A_{\frac{e-1}{2}} = \mathbb{Z}_p \setminus \{0\}$ 可得

$$\Delta_E(\mathcal{T}') = \Delta_E(\mathcal{T}) \setminus \left(\Delta_E\left(\mathbb{Z}_p \setminus (\{0\} \cup A_{\frac{e-1}{2}}), A_{\frac{e-1}{2}}\right) \cup \right. \\ \left. \Delta_E\left(A_{\frac{e-1}{2}}, \mathbb{Z}_p \setminus (\{0\} \cup A_{\frac{e-1}{2}})\right) \right).$$

由于

$$\Delta_E\left(A_{\frac{e-1}{2}}, \mathbb{Z}_p \setminus (\{0\} \cup A_{\frac{e-1}{2}})\right) \leq \underline{f}(\mathbb{Z}_p \setminus \{0\}),$$

$$\Delta_E\left(\mathbb{Z}_p \setminus \left(\{0\} \cup A_{\frac{e-1}{2}}\right), A_{\frac{e-1}{2}}\right) \leq f(\mathbb{Z}_p \setminus \{0\}),$$

再利用上式可得

$$\Delta_E(\mathcal{T}') \geq \frac{(p-3f-1)(\mathbb{Z}_p \setminus \{0\}) - 2f(\mathbb{Z}_p \setminus \{0\})}{(p-5f-1)(\mathbb{Z}_p \setminus \{0\})} =$$

综上可得, $\mathcal{T}'$ 是一个 $(p, 2f, (e-1)/2, p-5f-1)$ -DSS, 且冗余为 $r = 2f \cdot (e-1)/2 = ef - f$.

推论 2 当 $e \rightarrow \infty$ 时, $(p, 2f, (e-1)/2, p-5f-1)$ -DSS 是渐近最优的.

证明 由定理 2 中构造可知

$$\begin{aligned} \frac{t\rho(n-1)}{r^2(t-1)} &= \frac{(e-1)(ef+1-5f-1)(ef+1-1)}{(ef-f)^2(e-3)} = \\ &= \frac{(e-1)}{(e-3)} \cdot \frac{f(e-5)ef}{f^2(e-1)^2} = \\ &= \frac{(e-1)}{(e-3)} \cdot \left(1 - \frac{4}{e-1}\right) \left(1 + \frac{1}{e-1}\right). \end{aligned}$$

显然当 $e \rightarrow \infty$ 时, 有 $\lim_{e \rightarrow \infty} \frac{t\rho(n-1)}{r^2(t-1)} = 1$, 即所得

DSS 是渐近最优的.

设 s, m, l 是 3 个正整数满足 $m < l$. 设 $p = ef + 1$ 为素数满足 $e = ls + m$, 构造如下 $\mathbb{Z}_p$ 上的 $s + m$ 个子集:

$$\begin{aligned} A_0 &= \bigcup_{i=0}^{l-1} C_{is}^{(e,p)}, A_1 = \bigcup_{i=0}^{l-1} C_{is+1}^{(e,p)}, \dots, \\ A_{s-1} &= \bigcup_{i=0}^{l-1} C_{is+s-1}^{(e,p)}, A_s = C_{ls}^{(e,p)}, \\ A_{s+1} &= C_{ls+1}^{(e,p)}, \dots, A_{s+m-1} = C_{ls+m-1}^{(e,p)}. \end{aligned}$$

类似定理 1 的证明过程可以验证知:

由上述子集构造的集族 $\mathcal{T} = \{A_0, A_1, \dots, A_{s+m-1}\}$ 是一个 $(p, \{lf, \dots, lf, f, \dots, f\}, s+m, p-1-(l^2-l+1)f)$ -DSS. 因此, 可得如下结论.

定理 3 设 $p = ef + 1$ 为素数, s, m, l 是 3 个正整数, 满足 $e = ls + m, m < l$. 则存在一个 $(p, \{lf, \dots, lf, f, \dots, f\}, s+m, p-1-(l^2-l+1)f)$ -DSS, 且冗余为 $r = ef$.

推论 3 当 $s \rightarrow \infty$ 时, $(p, \{lf, \dots, lf, f, \dots, f\}, s+m, p-1-(l^2-l+1)f)$ -DSS 是渐近最优的.

证明 由定理 3 可知:

$$\begin{aligned} \frac{t\rho(n-1)}{r^2(t-1)} &= (s+m)(ef+1-1-(l^2-l+1)f) \cdot \\ &\quad \frac{(ef+1-1)}{f^2e^2(s+m-1)} = \frac{s+m}{s+m-1}. \end{aligned}$$

$$\begin{aligned} \frac{f(e-l^2+l-1)ef}{f^2e^2} &= \\ \frac{s+m}{s+m-1} \cdot \left(1 - \frac{l^2-l+1}{e}\right). \end{aligned}$$

显然当 $s \rightarrow \infty$ 时, 有 $e \rightarrow \infty$ 且 $\lim_{e \rightarrow \infty} \frac{t\rho(n-1)}{r^2(t-1)} = 1$.

即所得 DSS 是渐近最优的.

3 集合差系统的乘积构造

此节将展示由两个 DSS 产生的乘积构造, 该构造为文献[3]中主要构造的推广, 也是文献[11]中主要构造的拓展.

定理 4 假设存在一个 $\text{CDC}(v_1, k, \lambda)$ 上的划分型 (v_1, K_1, m_1, ρ_1) -DSS, $\mathcal{T} = \{A_1, A_2, \dots, A_{m_1}\}$ 和一个划分 $\mathbb{Z}_{v_2} \setminus \{0\}$ 的 (v_2, K_2, m_2, ρ_2) -DSS. 若存在子集 $S \subset [m_1]$ 使得 $\Delta\left(\bigcup_{i \in S} A_i, \bigcup_{j \in [m_1]} A_j\right) \geq \underline{\mu} \mathbb{Z}_{v_1}$, 则存在一个 $(v_1 v_2, K, m_1 m_2 + |S|, \rho)$ -DSS, 其中, $\rho = \min\{\rho_1 \cdot (v_2 - 1), \rho_2 \lambda + 2\mu\}$, $K = \{k_1 k_2 : k_1 \in K_1, k_2 \in K_2\} \cup \{A_i : i \in S\}$, 且冗余为 $r = k(v_2 - 1) + \sum_{i \in S} |A_i|$.

证明 设 $\mathcal{H} = \{B_1, B_2, \dots, B_{m_2}\}$ 是一个划分 $\mathbb{Z}_{v_2} \setminus \{0\}$ 的 (v_2, K_2, m_2, ρ_2) -DSS. 构造如下 $\mathbb{Z}_{v_1 v_2}$ 上的 $m_1 m_2 + |S|$ 个区组, 对于 $i = 1, \dots, m_1$ 和 $j = 1, \dots, m_2$, 令

$$\begin{aligned} D_{i,j} &= \{v_2 a + b : a \in A_i, b \in B_j\}, \\ D_{i,0} &= \{v_2 a : a \in A_i\}. \end{aligned}$$

定义集族

$$\begin{aligned} \mathcal{G} &= \{D_{i,j} : i = 1, \dots, m_1, j = 1, \dots, m_2\} \cup \\ &\quad \{D_{i,0} : i \in S\}. \end{aligned}$$

下面计算外差 $\Delta_E(\mathcal{G})$.

情况 1 计算差 $v_2 a$ ($a \neq 0$) 在 $\Delta_E(\mathcal{G})$ 中出现的次数.

由 $\mathcal{G}$ 的定义可知, 差 $v_2 a$ 出现于

$$\bigcup_{j=1}^{m_2} \bigcup_{1 \leq i \neq i' \leq m_1} \Delta_E(D_{i,j}, D_{i',j}) \cup \bigcup_{i,i' \in S, i \neq i'} \Delta_E(D_{i,0}, D_{i',0}).$$

由 $\mathcal{T}$ 是一个 (v_1, K_1, m_1, ρ_1) -DSS, 可知

$$\bigcup_{1 \leq i \neq i' \leq m_1} \Delta_E(A_i, A_{i'}) \geq \underline{\rho}_1(\mathbb{Z}_{v_1} \setminus \{0\}),$$

则

$$\bigcup_{j=1}^{m_2} \bigcup_{1 \leq i \neq i' \leq m_1} \Delta_E(D_{i,j}, D_{i',j}) =$$

$$\begin{aligned} & \bigcup_{j=1}^{m_2} \bigcup_{1 \leq i \neq i' \leq m_1} \{v_2(a-a') + b - b' : a \in A_i, \\ & a' \in A_{i'}, b, b' \in B_j\} \geq \\ & \frac{(v_2-1)}{1 \leq i \neq i' \leq m_1} \bigcup \{v_2(a-a') : a \in A_i, a' \in A_{i'}\} \geq \\ & \rho_1(v_2-1)(\mathbb{Z}_{v_1 v_2} \setminus \{0\}). \end{aligned}$$

因此, 差 $v_2 a, a=1, 2, \dots, v_1-1$ 在 $\Delta_E(\mathcal{G})$ 中出现了 $\rho_1(v_2-1)$ 次.

情况 2 计算差 $v_2 a + b (b \neq 0)$ 在 $\Delta_E(\mathcal{G})$ 中出现的次数.

由 $\mathcal{G}$ 的定义可知, 差 $v_2 a + b (b \neq 0)$ 出现于

$$\begin{aligned} & \bigcup_{i=1}^{m_1} \bigcup_{i'=1}^{m_1} \bigcup_{1 \leq j \neq j' \leq m_2} \Delta_E(D_{i,j}, D_{i',j'}) \cup \\ & \bigcup_{i'=1}^{m_1} \bigcup_{j=1}^{m_2} \bigcup_{i \in S} \Delta_E(D_{i,0}, D_{i',j}) \cup \\ & \bigcup_{i'=1}^{m_1} \bigcup_{j=1}^{m_2} \bigcup_{i \in S} \Delta_E(D_{i',j}, D_{i,0}). \end{aligned}$$

设 $A = \bigcup_{i=1}^{m_1} A_i$. 由 $A = \bigcup_{i=1}^{m_1} A_i$ 是一个 $\text{CDC}(v_1, k, \lambda)$, 可知 $k \geq \lambda$ 且 $\Delta_E(A, A) = k\{0\} \cup \Delta(A) \geq k\{0\} \cup \lambda(\mathbb{Z}_{v_1} \setminus \{0\}) \geq \lambda \mathbb{Z}_{v_1}$, 则

$$\begin{aligned} & \bigcup_{i=1}^{m_1} \bigcup_{i'=1}^{m_1} \{v_2(a-a') : a \in A_i, a' \in A_{i'}\} = \\ & \{v_2(a-a') : a \in A, a' \in A\} \geq \\ & \lambda \{v_2 a : a = 0, 1, \dots, v_1-1\}. \end{aligned} \quad (4)$$

再由条件

$$\Delta\left(\bigcup_{i \in S} A_i, \bigcup_{j \in [m_1]} A_j\right) = \Delta\left(\bigcup_{i \in S} A_i, A\right) \geq \mu \mathbb{Z}_{v_1},$$

可得:

$$\begin{aligned} & \bigcup_{i=1}^{m_1} \bigcup_{i' \in S} \{v_2(a-a') : a \in A_i, a' \in A_{i'}\} = \\ & \{v_2(a-a') : a \in A, a' \in \bigcup_{i' \in S} A_{i'}\} \geq \\ & \mu \{v_2 a : a = 0, 1, \dots, v_1-1\}, \end{aligned} \quad (5)$$

$$\begin{aligned} & \bigcup_{i=1}^{m_1} \bigcup_{i' \in S} \{v_2(a'-a) : a \in A_i, a' \in A_{i'}\} = \\ & \{v_2(a'-a) : a \in A, a' \in \bigcup_{i' \in S} A_{i'}\} \geq \\ & \mu \{v_2 a : a = 0, 1, \dots, v_1-1\}. \end{aligned} \quad (6)$$

因为 $\mathcal{H} = \{B_1, B_2, \dots, B_{m_2}\}$ 是一个 (v_2, K_2, m_2, ρ_2) -DSS, 所以

$$\bigcup_{1 \leq j \neq j' \leq m_2} \Delta_E(B_j, B_{j'}) \geq \rho_2(\mathbb{Z}_{v_2} \setminus \{0\}).$$

由等式(4)、(5)、(6)和 $\bigcup_{i=1}^{m_2} B_i = \mathbb{Z}_{v_2} \setminus \{0\}$ 可知,

$$\begin{aligned} & \bigcup_{i=1}^{m_1} \bigcup_{i'=1}^{m_1} \bigcup_{1 \leq j \neq j' \leq m_2} \Delta_E(D_{i,j}, D_{i',j'}) \cup \\ & \bigcup_{i'=1}^{m_1} \bigcup_{j=1}^{m_2} \bigcup_{i \in S} \Delta_E(D_{i,0}, D_{i',j}) \cup \\ & \bigcup_{i'=1}^{m_1} \bigcup_{j=1}^{m_2} \bigcup_{i \in S} \Delta_E(D_{i',j}, D_{i,0}) = \\ & \bigcup_{i=1}^{m_1} \bigcup_{i'=1}^{m_1} \bigcup_{1 \leq j \neq j' \leq m_2} \{v_2(a-a') + b - b' : a \in A_i, \\ & a' \in A_{i'}, b \in B_j, b' \in B_{j'}\} \cup \\ & \bigcup_{i'=1}^{m_1} \bigcup_{j=1}^{m_2} \bigcup_{i \in S} \{v_2(a-a') - b : a \in A_i, \\ & a' \in A_{i'}, b \in B_j\} \cup \\ & \bigcup_{i'=1}^{m_1} \bigcup_{j=1}^{m_2} \bigcup_{i \in S} \{v_2(a'-a) + b : a \in A_i, \\ & a' \in A_{i'}, b \in B_j\} \geq \\ & \bigcup_{1 \leq j \neq j' \leq m_2} \{v_2(a-a') + b - b' : a \in A, \\ & a' \in A, b \in B_j, b' \in B_{j'}\} \cup \\ & \{v_2(a-a') - b : a \in \bigcup_{i \in S} A_i, a' \in A, \\ & b=1, 2, \dots, v_2-1\} \cup \\ & \{v_2(a'-a) + b : a \in \bigcup_{i \in S} A_i, a' \in A, \\ & b=1, 2, \dots, v_2-1\} \geq \\ & (\rho_2 \lambda + 2\mu)(\mathbb{Z}_{v_1 v_2} \setminus v_2 \mathbb{Z}_{v_1 v_2}). \end{aligned}$$

因此, 差 $v_2 a + b (b \neq 0)$ 都在 $\Delta_E(\mathcal{G})$ 中出现了 $\rho_2 \lambda + 2\mu$ 次, 从而可得一个 $(v_1 v_2, K, m_1 m_2 + |S|, \rho)$ -DSS, 其中 $\rho = \min\{\rho_1(v_2-1), \rho_2 \lambda + 2\mu\}$, 冗余为

$$r = k(v_2-1) + \sum_{i \in S} |A_i|.$$

接下来将利用定理 4 来得到一些渐近最优的 DSS. 在此之前, 需要以下 3 个引理.

引理 3^[4] 设 $p = 2ef + 1 \equiv 3 \pmod{4}$ 是一个素数, 则 $\{C_0^{(2e, p)}, C_2^{(2e, p)}, \dots, C_{2e-2}^{(2e, p)}\}$ 是一个完美且正则的 $(p, f, e, f(e-1)/2)$ -DSS.

引理 4^[17] 设 $p \equiv 3 \pmod{4}$ 是一个素数, 则 $C_0^{(2, p)}$ 是一个 $\text{DS}(p, (p-1)/2, (p-3)/4)$.

引理 5^[8] 设 g 和 v 是 2 个正整数, 则

$$\Delta(\mathbb{Z}_{g^v} \setminus v\mathbb{Z}_{g^v}) = (\underline{gv} - 2g)(\mathbb{Z}_{g^v} \setminus v\mathbb{Z}_{g^v}) \cup$$

$$(\underline{gv-g})(v\mathbb{Z}_{gv} \setminus \{0\}).$$

因此, 对于 $\mathbb{Z}_{gv}$ 上的 t -CDP (gv, K, λ) $\mathcal{H} = \{B_0, B_1, \dots, B_{t-1}\}$, 若 $\mathcal{H}$ 中所有区组都不包含 $v\mathbb{Z}_{gv}$ 中的任意元素, 则称 $\mathcal{H}$ 为 (gv, g, K, λ) 循环相对差填充(cyclic relative difference packing, CRDP), 记为 (gv, g, K, λ) -CRDP. 若

$$\bigcup_{i=0}^{t-1} B_i = \mathbb{Z}_{gv} \setminus v\mathbb{Z}_{gv},$$

则称为划分型 (gv, g, K, λ) -CRDP.

定理 5 设 g 和 v 是 2 个正整数. 若 $\mathbb{Z}_{gv}$ 上存在一个区组数为 t 的划分型 (gv, g, K, λ) -CRDP, 则存在一个 $(gv, K, t, gv - \lambda - 2g)$ -DSS.

证明 设 $\mathcal{T} = \{A_0, A_1, \dots, A_{t-1}\}$ 是 $\mathbb{Z}_{gv}$ 上的划分型 (gv, g, K, λ) -CRDP, 由引理 5 可得

$$\bigcup_{i=0}^{t-1} A_i = \mathbb{Z}_{gv} \setminus v\mathbb{Z}_{gv}, \Delta(H) \leq \underline{\lambda}(\mathbb{Z}_{gv} \setminus v\mathbb{Z}_{gv}).$$

下面计算 $\Delta_E(\mathcal{T})$:

$$\begin{aligned} \Delta_E(\mathcal{T}) &= \Delta\left(\bigcup_{i=0}^{t-1} A_i\right) \setminus \Delta(\mathcal{T}) = \Delta(\mathbb{Z}_{gv} \setminus v\mathbb{Z}_{gv}) \setminus \\ &\quad \Delta(\mathcal{T}) \geq (\underline{gv-2g})(\mathbb{Z}_{gv} \setminus v\mathbb{Z}_{gv}) \cup \\ &\quad (\underline{gv-g})(v\mathbb{Z}_{gv} \setminus \{0\}) \setminus \underline{\lambda}(\mathbb{Z}_{gv} \setminus v\mathbb{Z}_{gv}) \geq \\ &\quad (\underline{gv-2g-\lambda})(\mathbb{Z}_{gv} \setminus v\mathbb{Z}_{gv}) \cup \\ &\quad (\underline{gv-g})(v\mathbb{Z}_{gv} \setminus \{0\}). \end{aligned}$$

又因为 $(gv-2g-\lambda) < (gv-g)$, 所以可得 $\mathcal{T}$ 是一个 $(gv, K, t, gv - \lambda - 2g)$ -DSS.

引理 6^[18] 设 v 的素因子分解为 $v = p_1^{t_1} p_2^{t_2} \dots p_l^{t_l}$, 其中 $p_1, \dots, p_l$ 是互不相同的素数. 设 $e > 1$ 是一个整数, 对每一个 $i, i = 1, \dots, l$ 都有 $e|(p_i - 1)$, 则存在一个划分型 $(v, 1, e, e-1)$ -CRDP.

引理 7^[18] 设 v 的素因子分解为 $v = p_1^{t_1} p_2^{t_2} \dots p_l^{t_l}$, 其中 $p_1, \dots, p_l$ 是互不相同的素数. 设 $e > 1$ 是一个整数, 对每一个 $i(i = 1, \dots, l)$ 都有 $e|(p_i - 1)$, 则存在一个划分型 (ev, e, e, e) -CRDP.

定理 6 设 $p' = 2e'f' + 1 \equiv 3(\text{mod } 4)$ 和 $p = ef + 1$ 为两个素数. 若 $e > 2e'$ 和 $f' \geq 2$, 则存在一个渐近最优 $(p'p, \{ff', \dots, ff', f', \dots, f'\}, e'e + e', \text{eff}'(e' - 1)/2)$ -DSS.

证明 由引理 1 可知, 集族 $\{C_0^{(e,p)}, C_1^{(e,p)}, \dots, C_{e-1}^{(e,p)}\}$ 是一个划分 $\mathbb{Z}_p \setminus \{0\}$ 的 $(p, f, e, f(e-1))$ -DSS. 由引理 3 知, 集族 $\{C_0^{(2e',p)}, C_2^{(2e',p)}, \dots, C_{2e'-2}^{(2e',p)}\}$

是一个 $(p', f', e', f'(e' - 1)/2)$ -DSS 且满足

$$\bigcup_{i=0}^{e'-1} C_i^{(2e',p)} = C_0^{(2,p)}.$$

由引理 4 知,

$$\begin{aligned} \Delta_E(C_0^{(2,p)}, C_0^{(2,p')}) &= \frac{p'-1}{2} \{0\} \cup \Delta(C_0^{(2,p')}) = \\ &\quad \frac{p'-1}{2} \{0\} \cup \frac{p'-3}{4} (\mathbb{Z}_{p'} \setminus \{0\}) \geq \frac{p'-3}{4} \mathbb{Z}_{p'}, \end{aligned}$$

取 $|S| = e'$, 可得 $\mu = (p' - 3)/4$, 再应用定理 4 可构造一个 $(p'p, \{ff', \dots, ff', f', \dots, f'\}, e'e + e', \rho)$ -DSS, 其中, $\rho = \min\{\text{eff}'(e' - 1)/2, (f'e' - 1)f(e - 1)/2 + f'e' - 1\}$, 由 $e > 2e'$ 和 $f' \geq 2$ 可得 $\rho = \text{eff}'(e' - 1)/2$. 由定理 4 可知, 此 DSS 的冗余为 $r = e'\text{eff}' + e'f'$. 则

$$\begin{aligned} \frac{t\rho(n-1)}{r^2(t-1)} &= \frac{(e'e + e')\text{eff}'(e' - 1)}{2(e'\text{eff}' + e'f')^2} \cdot \\ &\quad \frac{(2e'f' + 1)(ef + 1) - 1}{(e'e + e' - 1)} = \\ &\quad \frac{(e'e + e')}{(e'e + e' - 1)} \cdot \left(\left(1 - \frac{1}{e'}\right) \left(1 - \frac{1}{ef + 1}\right) + \right. \\ &\quad \left. \frac{1}{2e'f'} \left(1 - \frac{1}{ef + 1}\right)^2 \left(1 - \frac{1}{e'}\right) \right). \end{aligned}$$

显然当 $e', e \rightarrow \infty$ 时, 有 $\lim_{e', e \rightarrow \infty} \frac{t\rho(n-1)}{r^2(t-1)} = 1$. 即

所得 DSS 是渐近最优的.

定理 7 设 $p = 2ef + 1 \equiv 3(\text{mod } 4)$ 为一个素数. 设 v 的素因子分解为 $v = p_1^{t_1} p_2^{t_2} \dots p_l^{t_l}$, 其中 $p_1, \dots, p_l$ 是互不相同的素数. 设 $w > 1$ 是一个整数, 对每一个 $i(i = 1, \dots, l)$ 都有 $w|(p_i - 1)$. 若 $efw < (f - 1)v$, 则存在一个渐近最优的 $(pv, \{fw, \dots, fw, f, \dots, f\}, e(v-1)/w + e, (v-1)f(e-1)/2)$ -DSS.

证明 将定理 5 应用于引理 6 中的划分型 $(v, 1, w, w-1)$ -CRDP, 可得一个 $(v, w, (v-1)/w, v - w - 1)$ -DSS. 再由引理 3 知, 集族 $\{C_0^{(2e,p)}, C_2^{(2e,p)}, \dots, C_{2e-2}^{(2e,p)}\}$ 是一个 $(p, f, e, f(e-1)/2)$ -DSS 且满足

$$\bigcup_{i=0}^{e-1} C_i^{(2e,p)} = C_0^{(2,p)}.$$

利用引理 4 可得:

$$\begin{aligned} \Delta_E(C_0^{(2,p)}, C_0^{(2,p')}) &= \frac{p-1}{2} \{0\} \cup \Delta(C_0^{(2,p')}) = \\ &\quad \frac{p-1}{2} \{0\} \cup \frac{p-3}{4} (\mathbb{Z}_p \setminus \{0\}) \geq \frac{p-3}{4} \mathbb{Z}_p. \end{aligned}$$

取 $|S| = e$ 可得 $\mu = (p-3)/4$. 再应用定理 4 可构造得一个 $(p\nu, \{fw, \dots, fw, f, \dots, f\}, e(v-1)/w+e, \rho)$ -DSS, 其中

$\rho = \min\{(v-1)f(e-1)/2, (fe-1)(v-w+1)/2\}$, 由 $efw < (f-1)v$ 可得 $\rho = (v-1)f(e-1)/2$. 由定理 4 可知, 此 DSS 的冗余为 $r = efv$. 则

$$\begin{aligned} \frac{t\rho(n-1)}{r^2(t-1)} &= \frac{e(v-1)/w+e}{2e^2f^2v^2} \cdot \\ &\quad \frac{(v-1)f(e-1)((2fe+1)v-1)}{e(v-1)/w+e-1} = \\ &\quad \frac{e(v-1)/w+e}{e(v-1)/w+e-1} \cdot \\ &\quad \left(\frac{(v-1)(e-1)(2fe+1)v}{2e^2f^2v^2} - \frac{(v-1)(e-1)}{2e^2f^2v^2} \right) = \\ &\quad \frac{e(v-1)/w+e}{e(v-1)/w+e-1} \cdot \\ &\quad \left(\left(1-\frac{1}{v}\right)\left(1-\frac{1}{e}\right) + \frac{1}{2ef}\left(1-\frac{1}{v}\right)\left(1-\frac{1}{e}\right) \right). \end{aligned}$$

显然当 $e, v \rightarrow \infty$ 时, 有 $\lim_{e, v \rightarrow \infty} \frac{t\rho(n-1)}{r^2(t-1)} = 1$. 即所得 DSS 是渐近最优的.

定理 8 设 $p = ef + 1$ 为一个素数. 设 v 的素因子分解为 $v = p_1^{i_1} p_2^{i_2} \cdots p_l^{i_l}$, 其中 $p_1, \dots, p_l$ 是互不相同的素数. 设 $w > 1$ 是一个整数, 对每一个 i ($i = 1, \dots, l$) 都有 $w|(p_i - 1)$. 若 $v < e$, 则存在一个渐近最优的 $(wvp, \{fw, \dots, fw, w, \dots, w\}, (v-1)(e+1), (wv-3w)fe)$ -DSS.

证明 将定理 5 应用于引理 7 中的划分型 (wv, w, w, w) -CRDP, 可得一个 $(wv, w, v-1, wv-3w)$ -DSS. 再由引理 1 知, 集族 $\{C_0^{(e,p)}, C_1^{(e,p)}, \dots, C_{e-1}^{(e,p)}\}$ 是 $\mathbb{Z}_p \setminus \{0\}$ 上一个划分型 $(p, f, e, f(e-1))$ -DSS. 利用引理 5 可得

$$\begin{aligned} \Delta_E(\mathbb{Z}_{wv} \setminus w\mathbb{Z}_{wv}, \mathbb{Z}_{wv} \setminus w\mathbb{Z}_{wv}) &= \\ &\quad \frac{(wv-w)\{0\} \cup \Delta(\mathbb{Z}_{wv} \setminus w\mathbb{Z}_{wv})}{(wv-w)\{0\} \cup (wv-2w)(\mathbb{Z}_{wv} \setminus \{0\})} \geq \\ &\quad \frac{(wv-2w)\mathbb{Z}_{wv}}{(wv-2w)\mathbb{Z}_{wv}}. \end{aligned}$$

取 $|S| = v-1$, 可得 $\mu = wv-2w$. 再应用定理 4 构造可得 $(wvp, \{fw, \dots, fw, w, \dots, w\}, (v-1)(e+1), \rho)$ -DSS, 其中, $\rho = \min\{(wv-3w)fe, (wv-2w)(fe-f+2)\}$, 由 $v < e$ 可得 $\rho = (wv-3w)fe$. 由定理 4 可

知, 此 DSS 的冗余为 $r = (wv-w)(fe+1)$. 则

$$\begin{aligned} \frac{t\rho(n-1)}{r^2(t-1)} &= \frac{(v-1)(e+1)(wv-3w)}{((wv-w)(fe+1))^2} \cdot \\ &\quad \frac{fe(wv(fe+1)-1)}{(v-1)(e+1)-1} = \frac{(v-1)(e+1)}{(v-1)(e+1)-1} \cdot \\ &\quad \left(\frac{(wv-3w)fewv(fe+1)}{(wv-w)^2(fe+1)^2} - \right. \\ &\quad \left. \frac{(wv-3w)fe}{(wv-w)^2(fe+1)^2} \right) = \frac{(v-1)(e+1)}{(v-1)(e+1)-1} \cdot \\ &\quad \left(\left(1-\frac{2}{v-1}\right)\left(1+\frac{1}{v-1}\right)\left(1-\frac{1}{fe+1}\right) - \right. \\ &\quad \left. \frac{1}{(wv-w)(fe+1)}\left(1-\frac{2}{v-1}\right)\left(1-\frac{1}{fe+1}\right) \right). \end{aligned}$$

显然当 $e, v \rightarrow \infty$ 时, 有 $\lim_{e, v \rightarrow \infty} \frac{t\rho(n-1)}{r^2(t-1)} = 1$, 即所得 DSS 是渐近最优的.

参考文献:

- [1] LEVENSHTIN V I. One method of constructing quasilinear codes providing synchronization in the presence of errors[J]. Problems of Information Transmission, 1971, 7(3):215-222.
- [2] WANG H. A new bound for difference systems of sets[J]. Journal of Combinatorial Mathematics and Combinatorial Computing, 2006, 58:161-167.
- [3] CHISAKI S, KIMURA Y, MIYAMOTO N. A recursive construction for difference systems of sets[J]. Designs, Codes and Cryptography, 2019, 87(5):1059-1068.
- [4] TONCHEV V D. Difference systems of sets and code synchronization[J]. Rendiconti del Seminario Matematico di Messina: Serie II, 2003, 9:217-226.
- [5] TONCHEV V D. Partitions of difference sets and code synchronization[J]. Finite Fields and Their Applications, 2005, 11(3):601-621.
- [6] FUJI-HARA R, MUNEMASA A, TONCHEV V D. Hyperplane partitions and difference systems of sets[J]. Journal of Combinatorial Theory: Series A, 2006, 113(8): 1689-1698.
- [7] 范翠玲. 最优的集合差系统的构造[D]. 石家庄: 河北师范大学, 2010.
- [8] FAN C L, LEI J G, SHAN X L. Constructions of optimal difference systems of sets[J]. Science China Mathematics, 2011, 54(1):173-184.
- [9] QI M L, XIONG S W, YUAN J L, et al. On some new

- difference systems of sets constructed from the cyclotomic classes of order 12[J]. *Discrete Mathematics*, 2017, 340(10):2531-2537.
- [10] FUJIWARA Y, FUJIHARA R. Frequency hopping sequences with optimal auto-and cross-correlation properties and related codes[C]//10th International Workshop Algebraic Combinatorial Coding Theory, 2006: 83-96.
- [11] WANG X, WANG J H. Optimal difference systems of sets and difference sets[J]. *Aequationes Mathematicae*, 2011, 82(1/2):155-164.
- [12] FAN C L, LEI J G. Constructions of difference systems of sets from finite projective geometry[J]. *IEEE Transactions on Information Theory*, 2012, 58(1):130-138.
- [13] LEI J G, FAN C L. Optimal difference systems of sets and partition-type cyclic difference packings[J]. *Designs, Codes and Cryptography*, 2011, 58(2):135-153.
- [14] 王红瑞. 集合差系统的若干构造[D]. 石家庄: 河北师范大学, 2012.
- [15] REN W L, WANG F. A new class of optimal wide-gap one-coincidence frequency-hopping sequence sets[J]. *Advances in Mathematics of Communications*, 2023, 17(2):342-352.
- [16] YIN W J, XIANG C, FU F W. New frequency-hopping sequence sets with good parameters under aperiodic hamming correlation[J]. *Cryptography and Communications*, 2023, 15(1):159-169.
- [17] STORER T. *Cyclotomy and Difference Sets*[M]. Chicago: Markham Publishing Company, 1967.
- [18] BAO J J, JI L J. New families of optimal frequency hopping sequence sets[J]. *IEEE Transactions on Information Theory*, 2016, 62(9):5209-5224.

New constructions of difference systems of sets

SHEN Shuyu, BAO Jingjun

(School of Mathematics and Statistics, Ningbo University, Ningbo 315211, China)

Abstract: In this paper, we study new constructions of difference systems of sets. Two direct constructions of difference systems of sets are presented using cyclotomic classes over finite fields, and a new recursive construction of difference systems of sets is established using Kronecker product, which can be viewed as a generalization of the known constructions. By applying these direct and recursive constructions, some infinite series of asymptotically optimal difference systems of sets can be constructed.

Key words: difference system of sets; cyclotomic class; difference covering; code synchronization

(责任编辑 章践立)