Linear codes for SSS-based polynomial masking

The SSS-based masking is a special case of GCM (Generalized Code-based masking)

n = 3 shares, t = 2, q = 7 GMs (5,2)-SSS (Shamir's Secret Sharing)

Parameters:

- $\mathcal{Z} = \{\mathcal{Z} = \mathcal{F}_7 \times \mathcal{F}_7 \times \mathcal{F}_7\}$, $\mathcal{Z}_1 = \mathcal{F}_7 \times \mathcal{F}_7$, $\mathcal{Z}_2 = \mathcal{F}_7 \times \mathcal{F}_7$, $\mathcal{Z}_3 = \mathcal{F}_7 \times \mathcal{F}_7$, $\mathcal{F}_7 = \{\mathcal{F}_7 = \{0 = 0 \bmod 7, \ldots, 6 = 6 \bmod 7\}\}$; $|\mathcal{Z}| = 7^3 = 343$ elements $\mathcal{Z} = \{\mathcal{Z}_1, \mathcal{Z}_2\}$ and $\mathcal{Z}$ are the secret sharing domain, based on the previous work, respectively, where $\mathcal{Z}_1 \cap \mathcal{Z}_2 = \emptyset$; the three public points in GSS-scheme $\mathcal{P} = \{\mathcal{P}_1 = 1, \mathcal{P}_2 = 2, \mathcal{P}_3 = 3\}$; $\mathcal{P}_1 \cup \mathcal{P}_2 \cup \mathcal{P}_3 = \mathcal{P}$; $|\mathcal{P}| = 3$; $\mathcal{P}_1 \cap \mathcal{P}_2 \cap \mathcal{P}_3 = \emptyset$; $\mathcal{P}_1 = \{1\}$, $\mathcal{P}_2 = \{2\}$, $\mathcal{P}_3 = \{3\}$; $\mathcal{P}_1 \cup \mathcal{P}_2 = \{1, 2\}$, $\mathcal{P}_1 \cup \mathcal{P}_3 = \{1, 3\}$, $\mathcal{P}_2 \cup \mathcal{P}_3 = \{2, 3\}$; $\mathcal{P}_1 \cap \mathcal{P}_2 = \emptyset$, $\mathcal{P}_1 \cap \mathcal{P}_3 = \emptyset$, $\mathcal{P}_2 \cap \mathcal{P}_3 = \emptyset$
- $\mathcal{Z} = \{\mathcal{Z}_1, \mathcal{Z}_2\}$ and $\mathcal{Z}_1 = \{\mathcal{Z}_1 = \{0, 1, 2, 3, 4, 5, 6\}\}$ and $\mathcal{Z}_2 = \{\mathcal{Z}_2 = \{0, 1, 2, 3, 4, 5, 6\}\}$; $|\mathcal{Z}_1| = |\mathcal{Z}_2| = 7$; $|\mathcal{Z}_1| + |\mathcal{Z}_2| = 14$; $\mathcal{Z}_1 \cap \mathcal{Z}_2 = \emptyset$; $\mathcal{Z}_1 \cup \mathcal{Z}_2 = \mathcal{Z}$; $\mathcal{Z}_1 \cup \mathcal{Z}_2 = \{0, 1, 2, 3, 4, 5, 6\}$; $|\mathcal{Z}_1 \cup \mathcal{Z}_2| = 7$; $|\mathcal{Z}_1 \cup \mathcal{Z}_2| = |\mathcal{Z}_1| = |\mathcal{Z}_2|$; $\mathcal{Z}_1 \cup \mathcal{Z}_2 = \mathcal{Z}_1 = \mathcal{Z}_2$; $\mathcal{Z}_1 \cap \mathcal{Z}_2 = \emptyset$; $\mathcal{Z}_1 \cap \mathcal{Z}_2 = \emptyset$; $\mathcal{Z}_1 \cup \mathcal{Z}_2 = \mathcal{Z}