A Generalized Framework for Folding Codes and Applications to Proofs of Proximity

*International Workshop on **C**ode-**B**ased **Crypto**graphy, Zurich, Switzerland, May 25, 2024*

Adrien Pasquereau

University of St.Gallen
Institute of Computer Science

$P(x, w)$ $V(x)$

$\mathtt{Com}$ →

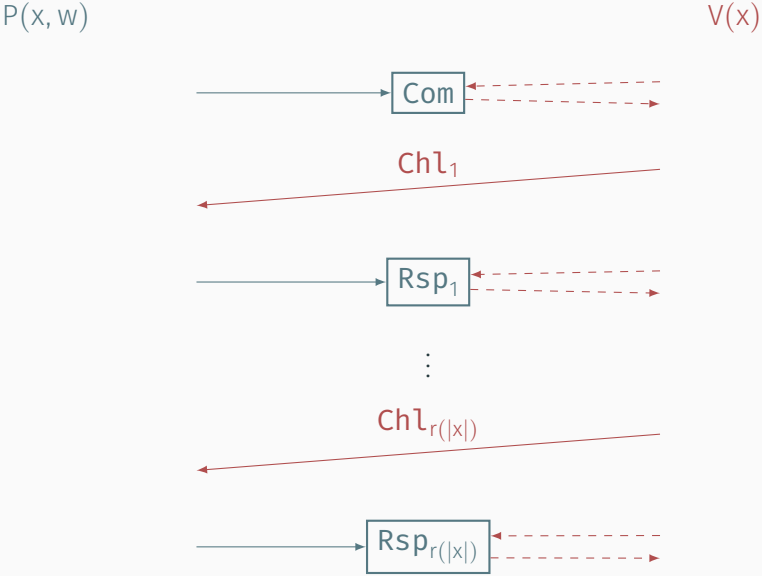
← $\mathtt{Chl}_1$

$\mathtt{Rsp}_1$ →

⋮

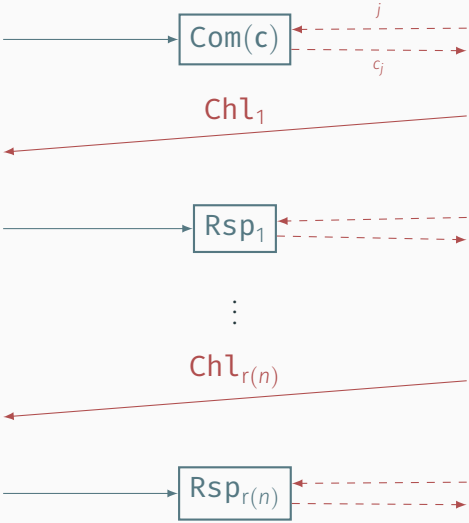
← $\mathtt{Chl}_{r(|x|)}$

$\mathtt{Rsp}_{r(|x|)}$ →


P(x, w)
V(x)
Com
Chl1
Rsp1
Chlr(|x|)
Rspr(|x|)

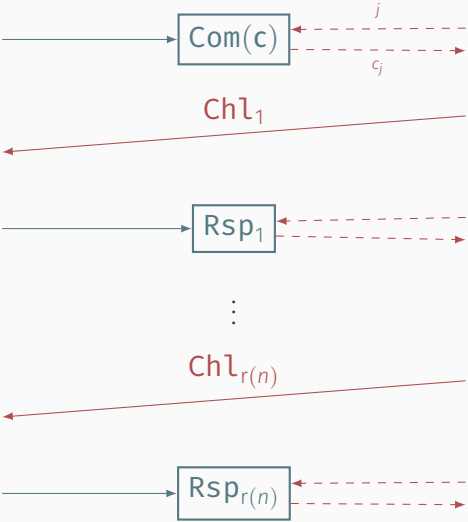
$\mathsf{P}((C \subseteq \mathbb{F}_q^n, \mathtt{Com}(\mathbf{c})), \mathbf{c} \in \mathbb{F}_q^n)$

$\mathsf{V}((C, \mathtt{Com}(\mathbf{c})))$



$\mathsf{P}((C \subseteq \mathbb{F}_q^n, \mathtt{Com}(\mathbf{c})), \mathbf{c} \in \mathbb{F}_q^n)$

$\mathsf{V}((C, \mathtt{Com}(\mathbf{c})))$



Accept (1) if $\mathbf{c} \in C$, otherwise Reject (0) with pb. $\geq 1 - \varepsilon(\frac{d(\mathbf{c},C)}{n})$.

Interactive Oracle Proofs (IOP) [Ben-Sasson, Chiesa, and Spooner 2016]

IP

An *interactive proof* system for a relation $\mathcal{R}$ with round complexity $r : \{0,1\}^* \to \mathbb{N}$ and soundness $\varepsilon : \{0,1\}^* \to [0,1]$ is a tuple (P, V), where P, V are probabilistic algorithms that satisfies the following properties.

- **Completeness**: For every $(x, w) \in \mathcal{R}$, $\langle P(x, w), V(w)\rangle$ is a transcript of $r(|x|)$ rounds and
$$\Pr\left[\langle P(x, w), V(x)\rangle \Rightarrow \mathbf{1}\right] = 1$$
- **Soundness**: For every $x \notin \mathcal{L}(\mathcal{R})$ and every $\tilde{P}$, $\langle \tilde{P}(x), V(w)\rangle$ is a transcript of $r(|x|)$ rounds and
$$\Pr\left[\langle \tilde{P}(x), V(x)\rangle \Rightarrow \mathbf{1}\right] \leq \varepsilon(x).$$

Interactive Oracle Proofs (IOP) [Ben-Sasson, Chiesa, and Spooner 2016]

IOP

An *interactive oracle proof* system for a relation $\mathcal{R}$ with round complexity $r : \{0,1\}^* \to \mathbb{N}$ and soundness $\varepsilon : \{0,1\}^* \to [0,1]$ is a tuple (P, V), where P, V are probabilistic algorithms that satisfies the following properties.

- **Completeness**: For every $(x, w) \in \mathcal{R}$, $\langle P(x, w), V(w)\rangle$ is a transcript of $r(|x|)$ rounds and
$$\Pr\left[\langle P(x, w), V(x)\rangle \Rightarrow \mathbf{1}\right] = 1$$
- **Soundness**: For every $x \notin \mathcal{L}(\mathcal{R})$ and every $\tilde{P}$, $\langle \tilde{P}(x), V(w)\rangle$ is a transcript of $r(|x|)$ rounds and
$$\Pr\left[\langle \tilde{P}(x), V(x)\rangle \Rightarrow \mathbf{1}\right] \leq \varepsilon(x).$$
- For every $x \in \{0,1\}^*$ and $0 \leq i \leq r(x)$, the i-th response of P is of the form $\mathtt{Rsp}_i = P(w, \{(j, \mathtt{Chl}_j)\}_{j<i}, \mathtt{state}_i)$ and the i-th challenge of V is of the form $\mathtt{Chl}_i = V^{\mathcal{O}_i(\mathtt{Rsp}_0,\ldots,\mathtt{Rsp}_i)}(x, \{(j, \mathtt{Chl}_j)\}_{j<i}, \mathtt{state}'_i)$.

What do we want? Why?

rounds complexity:	$\mathrm{r}(n)$
proof length:	$\mathrm{l}(n)$
query complexity:	$\mathrm{q}(n)$
prover complexity:	$\mathrm{t_P}(n)$
verifier complexity:	$\mathrm{t_V}(n)$

What do we want? Why?

rounds complexity:	$\mathsf{r}(n)$	$\leq \log(n)$
proof length:	$\mathsf{l}(n)$	$\leq O(n)$
query complexity:	$\mathsf{q}(n)$	$< O(n)$
prover complexity:	$\mathsf{t_P}(n)$	$\leq O(n)$
verifier complexity:	$\mathsf{t_V}(n)$	$< O(n)$

What do we want? Why?

rounds complexity:	$r(n)$	$\leq \log(n)$
proof length:	$l(n)$	$\leq O(n)$
query complexity:	$q(n)$	$< O(n)$
prover complexity:	$t_P(n)$	$\leq O(n)$
verifier complexity:	$t_V(n)$	$< O(n)$

Goal

Construct IOPP protocols with *sublinear* complexity (for the verifier) for *broad* families of codes.

Applications to...

- Succint Arguments: (zk-)SNARGs and (zk-)SNARKs,
- Non-Interactive Zero-Knowledge: compilers from SNARGs to (zk-)SNARGs and NIZKs,
- Integrity Verification: delegating computation to a non-trusted server over a network...

Table of contents

Motivation

Preliminaries

How do folding protocols work?

From the geometric intuition...

Generalized Framework

...to (linear) algebra and representation theory.

Preliminaries

How do folding protocols work?

The typical example: FRI [Ben-Sasson, Bentov, et al. 2017]

Let $\nu > \mathrm{r} \geq 0$, q an odd prime power such that $2^\nu | q-1$, $\alpha \in \mathbb{F}_q^\times$ with $\mathrm{ord}(\alpha) = 2^\nu$.
Set $n = 2^\nu$, $k = 2^{\mathrm{r}}$, $\mathcal{P} = \{\alpha^j \mid j \in \{0, \ldots, n-1\}\}$, and $C = \mathrm{RS}[\mathcal{P}, k]$.

For $f(X) = \sum_{i=0}^{m} f_i X^i \in \mathbb{F}_q[X]$, do we have $\deg f = m < k$?

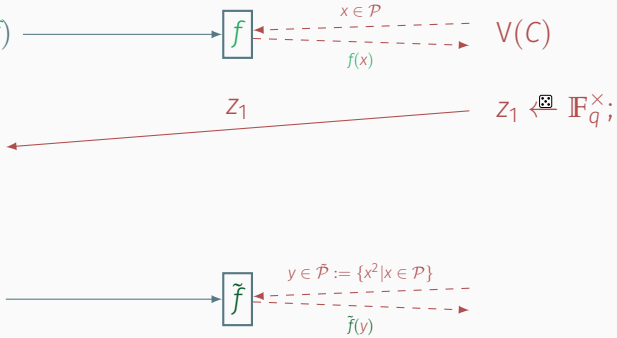
The typical example: FRI [Ben-Sasson, Bentov, et al. 2017]

$$f(X) = \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} f_{2i} X^{2i} + \sum_{i=0}^{\lfloor \frac{m-1}{2} \rfloor} f_{2i+1} X^{2i+1}$$

$$= \underbrace{\sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} f_{2i} (X^2)^i}_{g(X^2)} + X \underbrace{\sum_{i=0}^{\lfloor \frac{m-1}{2} \rfloor} f_{2i+1} (X^2)^i}_{h(X^2)};$$

$$\tilde{f}(Y) = \mathsf{Fold}[f, z_1](Y)$$

$$= g(Y) + z_1 h(Y);$$



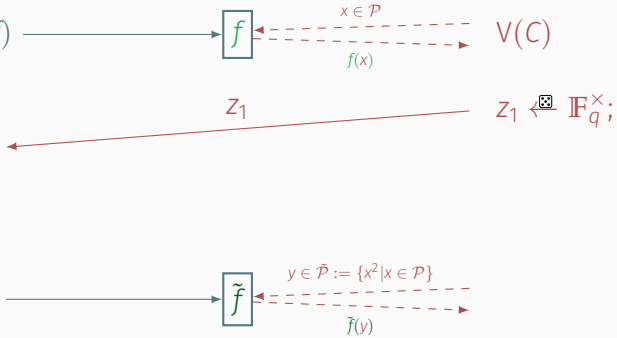
The typical example: FRI [Ben-Sasson, Bentov, et al. 2017]

$$f(X) = \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} f_{2i} X^{2i} + \sum_{i=0}^{\lfloor \frac{m-1}{2} \rfloor} f_{2i+1} X^{2i+1}$$

$$= \underbrace{\sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} f_{2i} (X^2)^i}_{g(X^2)} + X \underbrace{\sum_{i=0}^{\lfloor \frac{m-1}{2} \rfloor} f_{2i+1} (X^2)^i}_{h(X^2)};$$

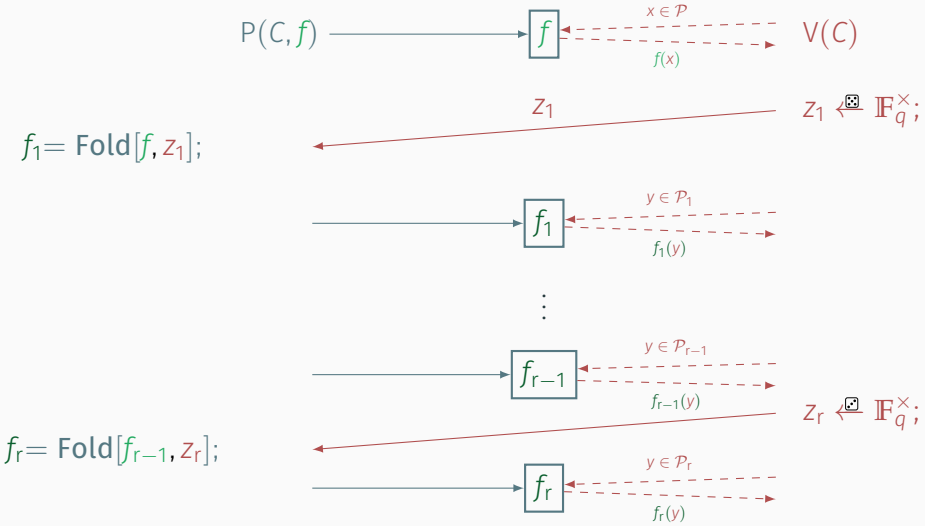
$$\tilde{f}(Y) = \mathbf{Fold}[f, z_1](Y)$$

$$= g(Y) + z_1 h(Y);$$



If $f \in C = \mathrm{RS}[\mathcal{P}, k]$, then $\tilde{f} = \mathbf{Fold}[f, z_1] \in \tilde{C} = \mathrm{RS}[\tilde{\mathcal{P}}, k/2]$.

The typical example: FRI [Ben-Sasson, Bentov, et al. 2017]



The typical example: FRI [Ben-Sasson, Bentov, et al. 2017]

Round consistency check for verification: For $y \neq 0$, verify whether

$$2 \cdot f_{i+1}(y^2) = (1 + z_1 y^{-1}) f_i(y) + (1 + z_i y^{-1}) f_i(-y),$$

which costs 1 query to f_{i+1} plus 2 queries to f_i.

Folding AG-Codes (intuition) [Bordage et al. 2020]

Suppose $N = \prod_{j=1}^{r-1} p_j$, let $\Gamma_0 = \Gamma \cong \mathbb{Z}/N\mathbb{Z}$, Γ_{i+1} such that $\Gamma_{i+1}/\Gamma_i \cong \mathbb{Z}/p_i\mathbb{Z}$, denote $\mathcal{X}_i : y^{\prod_{j=i}^{r-1} p_j} = \prod_{l=1}^{m}(x - a_l)$, $P_\infty^{(i)}$ the place at infinity on $\mathcal{X}_i$, $\pi_{i+1} : \mathcal{X}_i \to \mathcal{X}_{i+1}$.

[Proposition 29, Bordage et al. 2020]

Let $i \geq 0$. Set $D_i = d_i P_\infty^{(i)}$ for some integer d_i. Then $L_{\mathcal{X}_i}(D_i) = \bigoplus_{j=0}^{p_i-1} \nu_i^j \pi_i^*(L_{\mathcal{X}_{i-1}}(E_{i,j}))$ with $E_{i,j} = \left\lfloor \frac{1}{p_i} \pi_{i*}(D_i - j \cdot \mathrm{Div}_{\mathcal{X}_i}((\nu_i))) \right\rfloor$, for $0 \leq j \leq p_i - 1$, and some well chosen balancing function $\nu_i \in \mathbb{F}_q(\mathcal{X}_i)$ "compatible" with D_i.

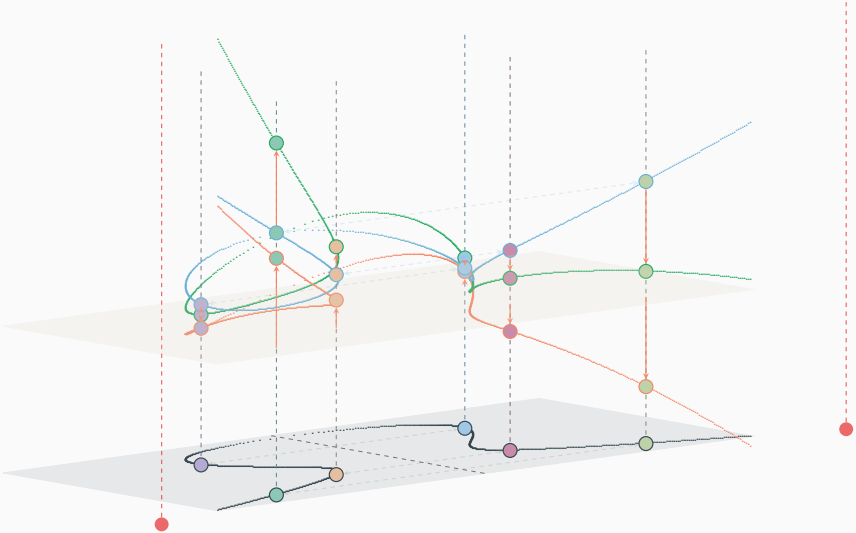
Corollary for real-world purposes

If $C = C(\mathcal{X}, \mathcal{P}, D)$ with $\mathcal{P} \subset \mathcal{X}$ a disjoint union of Γ-orbits of maximum size and D a Γ-invariant divisor, then for any $\mathbf{z} = (z_1, z_2) \in \mathbb{F}_q$, the operator $\mathbf{Fold}[f, \mathbf{z}] = \sum_{j=0}^{p_i-1} z_1^j f_j + \sum_{j=0}^{p_i-1} z_2^{j+1} \nu_{i+1,j} f_j$ induces a projection from $C(\mathcal{X}_i, \mathcal{P}_i, D_i)$ to $C(\mathcal{X}_i/\Gamma_i, \pi_{i+1}(\mathcal{P}_i), E_i)$, resulting in an *efficient* IOPP protocol.

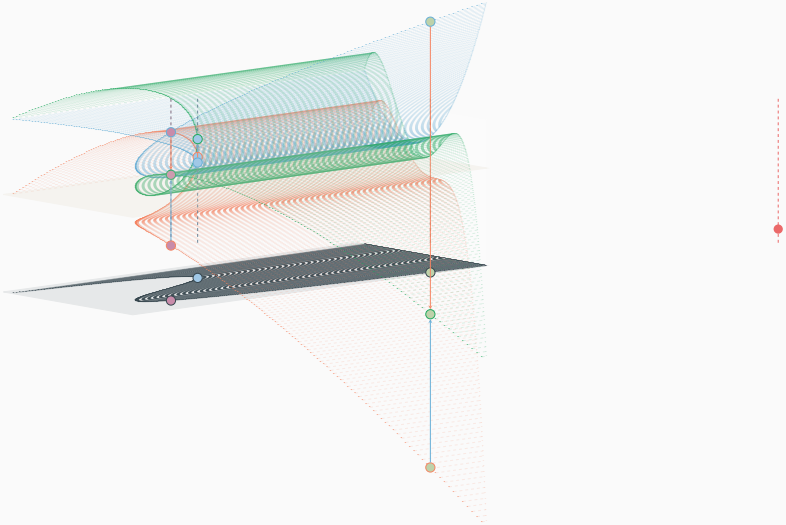
Preliminaries

From the geometric intuition...

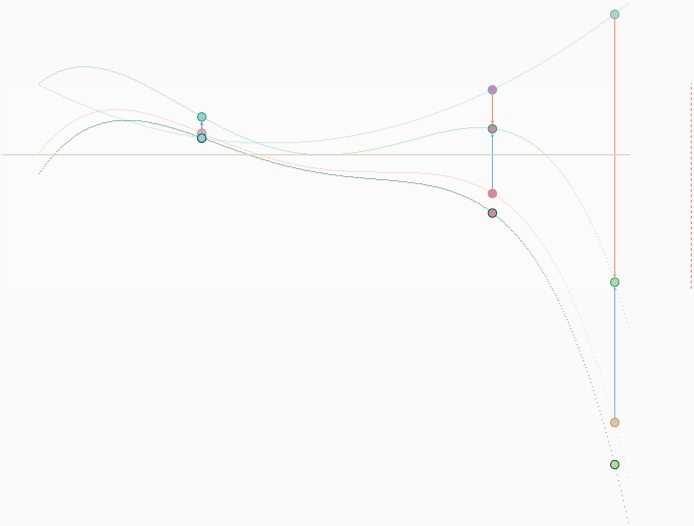
Geometric Intuition: Starting Curve



Geometric Intuition: Quotient Curve



Geometric Intuition: New Codeword



Generalized Framework

...to (linear) algebra and representation theory.

Staring at this generator matrix of an $[36, 14]_{37}$-code

$$\begin{pmatrix}
9 & 9 & 9 & 9 & 26 & 26 & 26 & 26 & 7 & 7 & 7 & 7 & 1 & 1 & 1 & 1 & 26 & 26 & 26 & 26 & 16 & 16 & 16 & 16 & 34 & 34 & 34 & 34 & 9 & 9 & 9 & 9 & 16 & 16 & 16 & 16 \\
7 & 7 & 7 & 7 & 17 & 17 & 17 & 17 & 13 & 13 & 13 & 13 & 4 & 4 & 4 & 4 & 35 & 35 & 35 & 35 & 32 & 32 & 32 & 32 & 6 & 6 & 6 & 6 & 8 & 8 & 8 & 8 & 34 & 34 & 34 & 34 \\
26 & 26 & 26 & 26 & 4 & 4 & 4 & 4 & 3 & 3 & 3 & 3 & 16 & 16 & 16 & 16 & 3 & 3 & 3 & 3 & 27 & 27 & 27 & 27 & 25 & 25 & 25 & 25 & 3 & 3 & 3 & 3 & 26 & 26 & 26 & 26 \\
12 & 12 & 12 & 12 & 14 & 14 & 14 & 14 & 32 & 32 & 32 & 32 & 27 & 27 & 27 & 27 & 14 & 14 & 14 & 14 & 17 & 17 & 17 & 17 & 24 & 24 & 24 & 24 & 15 & 15 & 15 & 15 & 9 & 9 & 9 & 9 \\
34 & 34 & 34 & 34 & 12 & 12 & 12 & 12 & 33 & 33 & 33 & 33 & 34 & 34 & 34 & 34 & 16 & 16 & 16 & 16 & 34 & 34 & 34 & 34 & 26 & 26 & 26 & 26 & 1 & 1 & 1 & 1 & 33 & 33 & 33 & 33 \\
8 & 11 & 29 & 26 & 1 & 6 & 36 & 31 & 10 & 23 & 27 & 14 & 1 & 6 & 36 & 31 & 1 & 6 & 36 & 31 & 8 & 11 & 29 & 26 & 10 & 23 & 27 & 14 & 8 & 11 & 29 & 26 & 8 & 11 & 29 & 26 \\
35 & 25 & 2 & 12 & 22 & 21 & 15 & 16 & 8 & 11 & 29 & 26 & 4 & 24 & 33 & 13 & 17 & 28 & 20 & 9 & 16 & 22 & 21 & 15 & 17 & 28 & 20 & 9 & 3 & 18 & 34 & 19 & 17 & 28 & 20 & 9 \\
19 & 3 & 18 & 34 & 3 & 18 & 34 & 19 & 36 & 31 & 1 & 6 & 16 & 22 & 21 & 15 & 30 & 32 & 7 & 5 & 32 & 7 & 5 & 30 & 3 & 18 & 34 & 19 & 15 & 16 & 22 & 21 & 13 & 4 & 24 & 33 \\
23 & 27 & 14 & 10 & 29 & 26 & 8 & 11 & 14 & 10 & 23 & 27 & 27 & 14 & 10 & 23 & 29 & 26 & 8 & 11 & 27 & 14 & 10 & 23 & 31 & 1 & 6 & 36 & 1 & 6 & 36 & 31 & 23 & 27 & 14 & 10 \\
3 & 34 & 3 & 34 & 10 & 27 & 10 & 27 & 9 & 28 & 9 & 28 & 1 & 36 & 1 & 36 & 10 & 27 & 10 & 27 & 4 & 33 & 4 & 33 & 16 & 21 & 16 & 21 & 3 & 34 & 3 & 34 & 4 & 33 & 4 & 33 \\
27 & 10 & 27 & 10 & 35 & 2 & 35 & 2 & 22 & 15 & 22 & 15 & 4 & 33 & 4 & 33 & 22 & 15 & 22 & 15 & 8 & 29 & 8 & 29 & 5 & 32 & 5 & 32 & 15 & 22 & 15 & 22 & 27 & 10 & 27 & 10 \\
21 & 16 & 21 & 16 & 30 & 7 & 30 & 7 & 25 & 12 & 25 & 12 & 16 & 21 & 16 & 21 & 4 & 33 & 4 & 33 & 16 & 21 & 16 & 21 & 27 & 10 & 27 & 10 & 1 & 36 & 1 & 36 & 25 & 12 & 25 & 12 \\
15 & 21 & 22 & 16 & 26 & 29 & 11 & 8 & 34 & 18 & 3 & 19 & 1 & 31 & 36 & 6 & 26 & 29 & 11 & 8 & 2 & 25 & 35 & 12 & 33 & 24 & 4 & 13 & 15 & 21 & 22 & 16 & 2 & 25 & 35 & 12 \\
24 & 4 & 13 & 33 & 17 & 9 & 20 & 28 & 5 & 7 & 32 & 30 & 4 & 13 & 33 & 24 & 35 & 12 & 2 & 25 & 4 & 13 & 33 & 24 & 8 & 26 & 29 & 11 & 1 & 31 & 36 & 6 & 32 & 30 & 5 & 7
\end{pmatrix}$$

Staring at this generator matrix of an $[36, 14]_{37}$-code

$$
\begin{pmatrix}
9 & 9 & 9 & 9 & 26 & 26 & 26 & 26 & 7 & 7 & 7 & 7 & 1 & 1 & 1 & 1 & 26 & 26 & 26 & 26 & 16 & 16 & 16 & 16 & 34 & 34 & 34 & 34 & 9 & 9 & 9 & 9 & 16 & 16 & 16 & 16 \\
7 & 7 & 7 & 7 & 17 & 17 & 17 & 17 & 13 & 13 & 13 & 13 & 4 & 4 & 4 & 4 & 35 & 35 & 35 & 35 & 32 & 32 & 32 & 32 & 6 & 6 & 6 & 6 & 8 & 8 & 8 & 8 & 34 & 34 & 34 & 34 \\
26 & 26 & 26 & 26 & 4 & 4 & 4 & 4 & 3 & 3 & 3 & 3 & 16 & 16 & 16 & 16 & 3 & 3 & 3 & 3 & 27 & 27 & 27 & 27 & 25 & 25 & 25 & 25 & 3 & 3 & 3 & 3 & 26 & 26 & 26 & 26 \\
12 & 12 & 12 & 12 & 14 & 14 & 14 & 14 & 32 & 32 & 32 & 32 & 27 & 27 & 27 & 27 & 14 & 14 & 14 & 14 & 17 & 17 & 17 & 17 & 24 & 24 & 24 & 24 & 15 & 15 & 15 & 15 & 9 & 9 & 9 & 9 \\
34 & 34 & 34 & 34 & 12 & 12 & 12 & 12 & 33 & 33 & 33 & 33 & 34 & 34 & 34 & 34 & 16 & 16 & 16 & 16 & 34 & 34 & 34 & 34 & 26 & 26 & 26 & 26 & 1 & 1 & 1 & 1 & 33 & 33 & 33 & 33 \\
8 & 11 & 29 & 26 & 1 & 6 & 36 & 31 & 10 & 23 & 27 & 14 & 1 & 6 & 36 & 31 & 1 & 6 & 36 & 31 & 8 & 11 & 29 & 26 & 10 & 23 & 27 & 14 & 8 & 11 & 29 & 26 & 8 & 11 & 29 & 26 \\
35 & 25 & 2 & 12 & 22 & 21 & 15 & 16 & 8 & 11 & 29 & 26 & 4 & 24 & 33 & 13 & 17 & 28 & 20 & 9 & 16 & 22 & 21 & 15 & 17 & 28 & 20 & 9 & 3 & 18 & 34 & 19 & 17 & 28 & 20 & 9 \\
19 & 3 & 18 & 34 & 3 & 18 & 34 & 19 & 36 & 31 & 1 & 6 & 16 & 22 & 21 & 15 & 30 & 32 & 7 & 5 & 32 & 7 & 5 & 30 & 3 & 18 & 34 & 19 & 15 & 16 & 22 & 21 & 13 & 4 & 24 & 33 \\
23 & 27 & 14 & 10 & 29 & 26 & 8 & 11 & 14 & 10 & 23 & 27 & 27 & 14 & 10 & 23 & 29 & 26 & 8 & 11 & 27 & 14 & 10 & 23 & 31 & 1 & 6 & 36 & 1 & 6 & 36 & 31 & 23 & 27 & 14 & 10 \\
3 & 34 & 3 & 34 & 10 & 27 & 10 & 27 & 9 & 28 & 9 & 28 & 1 & 36 & 1 & 36 & 10 & 27 & 10 & 27 & 4 & 33 & 4 & 33 & 16 & 21 & 16 & 21 & 3 & 34 & 3 & 34 & 4 & 33 & 4 & 33 \\
27 & 10 & 27 & 10 & 35 & 2 & 35 & 2 & 22 & 15 & 22 & 15 & 4 & 33 & 4 & 33 & 22 & 15 & 22 & 15 & 8 & 29 & 8 & 29 & 5 & 32 & 5 & 32 & 15 & 22 & 15 & 22 & 27 & 10 & 27 & 10 \\
21 & 16 & 21 & 16 & 30 & 7 & 30 & 7 & 25 & 12 & 25 & 12 & 16 & 21 & 16 & 21 & 4 & 33 & 4 & 33 & 16 & 21 & 16 & 21 & 27 & 10 & 27 & 10 & 1 & 36 & 1 & 36 & 25 & 12 & 25 & 12 \\
15 & 21 & 22 & 16 & 26 & 29 & 11 & 8 & 34 & 18 & 3 & 19 & 1 & 31 & 36 & 6 & 26 & 29 & 11 & 8 & 2 & 25 & 35 & 12 & 33 & 24 & 4 & 13 & 15 & 21 & 22 & 16 & 2 & 25 & 35 & 12 \\
24 & 4 & 13 & 33 & 17 & 9 & 20 & 28 & 5 & 7 & 32 & 30 & 4 & 13 & 33 & 24 & 35 & 12 & 2 & 25 & 4 & 13 & 33 & 24 & 8 & 26 & 29 & 11 & 1 & 31 & 36 & 6 & 32 & 30 & 5 & 7
\end{pmatrix}
$$

Staring at this generator matrix of an $[36, 14]_{37}$-code

9	9	9	9	26	26	26	26	7	7	7	7	1	1	1	1	26	26	26	26	16	16	16	16	34	34	34	34	9	9	9	9	16	16	16	16
7	7	7	7	17	17	17	17	13	13	13	13	4	4	4	4	35	35	35	35	32	32	32	32	6	6	6	6	8	8	8	8	34	34	34	34
26	26	26	26	4	4	4	4	3	3	3	3	16	16	16	16	3	3	3	3	27	27	27	27	25	25	25	25	3	3	3	3	26	26	26	26
12	12	12	12	14	14	14	14	32	32	32	32	27	27	27	27	14	14	14	14	17	17	17	17	24	24	24	24	15	15	15	15	9	9	9	9
34	34	34	34	12	12	12	12	33	33	33	33	34	34	34	34	16	16	16	16	34	34	34	34	26	26	26	26	1	1	1	1	33	33	33	33
8	11	29	26	1	6	36	31	10	23	27	14	1	6	36	31	1	6	36	31	8	11	29	26	10	23	27	14	8	11	29	26	8	11	29	26
35	25	2	12	22	21	15	16	8	11	29	26	4	24	33	13	17	28	20	9	16	22	21	15	17	28	20	9	3	18	34	19	17	28	20	9
19	3	18	34	3	18	34	19	36	31	1	6	16	22	21	15	30	32	7	5	32	7	5	30	3	18	34	19	15	16	22	21	13	4	24	33
23	27	14	10	29	26	8	11	14	10	23	27	27	14	10	23	29	26	8	11	27	14	10	23	31	1	6	36	1	6	36	31	23	27	14	10
3	34	3	34	10	27	10	27	9	28	9	28	1	36	1	36	10	27	10	27	4	33	4	33	16	21	16	21	3	34	3	34	4	33	4	33
27	10	27	10	35	2	35	2	22	15	22	15	4	33	4	33	22	15	22	15	8	29	8	29	5	32	5	32	15	22	15	22	27	10	27	10
21	16	21	16	30	7	30	7	25	12	25	12	16	21	16	21	4	33	4	33	16	21	16	21	27	10	27	10	1	36	1	36	25	12	25	12
15	21	22	16	26	29	11	8	34	18	3	19	1	31	36	6	26	29	11	8	2	25	35	12	33	24	4	13	15	21	22	16	2	25	35	12
24	4	13	33	17	9	20	28	5	7	32	30	4	13	33	24	35	12	2	25	4	13	33	24	8	26	29	11	1	31	36	6	32	30	5	7

Staring at this generator matrix of an $[36, 14]_{37}$-code

9	9	9	9	26	26	26	26	7	7	7	7	1	1	1	1	26	26	26	26	16	16	16	16	34	34	34	34	9	9	9	9	16	16	16	16
7	7	7	7	17	17	17	17	13	13	13	13	4	4	4	4	35	35	35	35	32	32	32	32	6	6	6	6	8	8	8	8	34	34	34	34
26	26	26	26	4	4	4	4	3	3	3	3	16	16	16	16	3	3	3	3	27	27	27	27	25	25	25	25	3	3	3	3	26	26	26	26
12	12	12	12	14	14	14	14	32	32	32	32	27	27	27	27	14	14	14	14	17	17	17	17	24	24	24	24	15	15	15	15	9	9	9	9
34	34	34	34	12	12	12	12	33	33	33	33	34	34	34	34	16	16	16	16	34	34	34	34	26	26	26	26	1	1	1	1	33	33	33	33
8	11	29	26	1	6	36	31	10	23	27	14	1	6	36	31	1	6	36	31	8	11	29	26	10	23	27	14	8	11	29	26	8	11	29	26
35	25	2	12	22	21	15	16	8	11	29	26	4	24	33	13	17	28	20	9	16	22	21	15	17	28	20	9	3	18	34	19	17	28	20	9
19	3	18	34	3	18	34	19	36	31	1	6	16	22	21	15	30	32	7	5	32	7	5	30	3	18	34	19	15	16	22	21	13	4	24	33
23	27	14	10	29	26	8	11	14	10	23	27	27	14	10	23	29	26	8	11	27	14	10	23	31	1	6	36	1	6	36	31	23	27	14	10
3	34	3	34	10	27	10	27	9	28	9	28	1	36	1	36	10	27	10	27	4	33	4	33	16	21	16	21	3	34	3	34	4	33	4	33
27	10	27	10	35	2	35	2	22	15	22	15	4	33	4	33	22	15	22	15	8	29	8	29	5	32	5	32	15	22	15	22	27	10	27	10
21	16	21	16	30	7	30	7	25	12	25	12	16	21	16	21	4	33	4	33	16	21	16	21	27	10	27	10	1	36	1	36	25	12	25	12
15	21	22	16	26	29	11	8	34	18	3	19	1	31	36	6	26	29	11	8	2	25	35	12	33	24	4	13	15	21	22	16	2	25	35	12
24	4	13	33	17	9	20	28	5	7	32	30	4	13	33	24	35	12	2	25	4	13	33	24	8	26	29	11	1	31	36	6	32	30	5	7

Staring at this generator matrix of an $[36, 14]_{37}$-code

9	9	9	9	26	26	26	26	7	7	7	7	1	1	1	1	26	26	26	26	16	16	16	16	34	34	34	34	9	9	9	9	16	16	16	16
7	7	7	7	17	17	17	17	13	13	13	13	4	4	4	4	35	35	35	35	32	32	32	32	6	6	6	6	8	8	8	8	34	34	34	34
26	26	26	26	4	4	4	4	3	3	3	3	16	16	16	16	3	3	3	3	27	27	27	27	25	25	25	25	3	3	3	3	26	26	26	26
12	12	12	12	14	14	14	14	32	32	32	32	27	27	27	27	14	14	14	14	17	17	17	17	24	24	24	24	15	15	15	15	9	9	9	9
34	34	34	34	12	12	12	12	33	33	33	33	34	34	34	34	16	16	16	16	34	34	34	34	26	26	26	26	1	1	1	1	33	33	33	33
8	11	29	26	1	6	36	31	10	23	27	14	1	6	36	31	1	6	36	31	8	11	29	26	10	23	27	14	8	11	29	26	8	11	29	26
35	25	2	12	22	21	15	16	8	11	29	26	4	24	33	13	17	28	20	9	16	22	21	15	17	28	20	9	3	18	34	19	17	28	20	9
19	3	18	34	3	18	34	19	36	31	1	6	16	22	21	15	30	32	7	5	32	7	5	30	3	18	34	19	15	16	22	21	13	4	24	33
23	27	14	10	29	26	8	11	14	10	23	27	27	14	10	23	29	26	8	11	27	14	10	23	31	1	6	36	1	6	36	31	23	27	14	10
3	34	3	34	10	27	10	27	9	28	9	28	1	36	1	36	10	27	10	27	4	33	4	33	16	21	16	21	3	34	3	34	4	33	4	33
27	10	27	10	35	2	35	2	22	15	22	15	4	33	4	33	22	15	22	15	8	29	8	29	5	32	5	32	15	22	15	22	27	10	27	10
21	16	21	16	30	7	30	7	25	12	25	12	16	21	16	21	4	33	4	33	16	21	16	21	27	10	27	10	1	36	1	36	25	12	25	12
15	21	22	16	26	29	11	8	34	18	3	19	1	31	36	6	26	29	11	8	2	25	35	12	33	24	4	13	15	21	22	16	2	25	35	12
24	4	13	33	17	9	20	28	5	7	32	30	4	13	33	24	35	12	2	25	4	13	33	24	8	26	29	11	1	31	36	6	32	30	5	7

Staring at this generator matrix of an $[18, 8]_{37}$-code

9	9	9	9	26	26	26	26	7	7	7	7	1	1	1	1	26	26	26	26	16	16	16	16	34	34	34	34	9	9	9	9	16	16	16	16
7	7	7	7	17	17	17	17	13	13	13	13	4	4	4	4	35	35	35	35	32	32	32	32	6	6	6	6	8	8	8	8	34	34	34	34
26	26	26	26	4	4	4	4	3	3	3	3	16	16	16	16	3	3	3	3	27	27	27	27	25	25	25	25	3	3	3	3	26	26	26	26
12	12	12	12	14	14	14	14	32	32	32	32	27	27	27	27	14	14	14	14	17	17	17	17	24	24	24	24	15	15	15	15	9	9	9	9
34	34	34	34	12	12	12	12	33	33	33	33	34	34	34	34	16	16	16	16	34	34	34	34	26	26	26	26	1	1	1	1	33	33	33	33
8	11	29	26	1	6	36	31	10	23	27	14	1	6	36	31	1	6	36	31	8	11	29	26	10	23	27	14	8	11	29	26	8	11	29	26
35	25	2	12	22	21	15	16	8	11	29	26	4	24	33	13	17	28	20	9	16	22	21	15	17	28	20	9	3	18	34	19	17	28	20	9
19	3	18	34	3	18	34	19	36	31	1	6	16	22	21	15	30	32	7	5	32	7	5	30	3	18	34	19	15	16	22	21	13	4	24	33
23	27	14	10	29	26	8	11	14	10	23	27	27	14	10	23	29	26	8	11	27	14	10	23	31	1	6	36	1	6	36	31	23	27	14	10
3	34	3	34	10	27	10	27	9	28	9	28	1	36	1	36	10	27	10	27	4	33	4	33	16	21	16	21	3	34	3	34	4	33	4	33
27	10	27	10	35	2	35	2	22	15	22	15	4	33	4	33	22	15	22	15	8	29	8	29	5	32	5	32	15	22	15	22	27	10	27	10
21	16	21	16	30	7	30	7	25	12	25	12	16	21	16	21	4	33	4	33	16	21	16	21	27	10	27	10	1	36	1	36	25	12	25	12
15	21	22	16	26	29	11	8	34	18	3	19	1	31	36	6	26	29	11	8	2	25	35	12	33	24	4	13	15	21	22	16	2	25	35	12
24	4	13	33	17	9	20	28	5	7	32	30	4	13	33	24	35	12	2	25	4	13	33	24	8	26	29	11	1	31	36	6	32	30	5	7

Commutator Relation

Let $G \in \mathbb{F}_{37}^{14\times 36}$ be the generator matrix from before.

What information can we get from relations of the form $LG = GR$ for $(L, R) \in \mathrm{GL}_k(\mathbb{F}_q) \times \mathrm{GL}_n(\mathbb{F}_q)$?

Commutator Relation

$$L_2 G = G R_2$$

for

$$L_2 = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 36
\end{pmatrix},$$

$$R_2 = \begin{pmatrix}
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}.$$

As left-representation?...

$$L_2 = P_2 D_2 P_2^{-1}$$

$$= \begin{pmatrix}
0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0
\end{pmatrix}
\begin{pmatrix}
36&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&36&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&36&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&36&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&36&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&36&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1
\end{pmatrix}
\begin{pmatrix}
0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0
\end{pmatrix}.$$

… as right-representation?…

$$R_2 = Q_2 E_2 Q_2^{-1}$$

$$= \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}
\begin{pmatrix}
36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 36 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}
\begin{pmatrix}
19 & 0 & 18 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 19 & 0 & 18 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 19 & 0 & 18 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 19 & 0 & 18 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 18 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 18 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 18 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 18 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 18 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 18 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 18 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 18 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 18 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 18 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 18 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 18 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 18 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 18 \\
19 & 0 & 19 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 19 & 0 & 19 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 19 & 0 & 19 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 19 & 0 & 19 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 19 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 19 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 19 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 19 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 19 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 19 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 19 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 19 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 19 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 19 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 19 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 19 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 19 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 19 & 0 & 19
\end{pmatrix}.$$

...and as a pair of representations!

$$P_2{}^{-1}GQ_2 = 2 \cdot \begin{pmatrix}
8 & 11 & 1 & 6 & 10 & 23 & 1 & 6 & 1 & 6 & 8 & 11 & 10 & 23 & 8 & 11 & 8 & 11 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
35 & 25 & 22 & 21 & 8 & 11 & 4 & 24 & 17 & 28 & 16 & 22 & 17 & 28 & 3 & 18 & 17 & 28 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
19 & 3 & 3 & 18 & 36 & 31 & 16 & 22 & 30 & 32 & 32 & 7 & 3 & 18 & 15 & 16 & 13 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
23 & 27 & 29 & 26 & 14 & 10 & 27 & 14 & 29 & 26 & 27 & 14 & 31 & 1 & 1 & 6 & 23 & 27 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
15 & 21 & 26 & 29 & 34 & 18 & 1 & 31 & 26 & 29 & 2 & 25 & 33 & 24 & 15 & 21 & 2 & 25 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
24 & 4 & 17 & 9 & 5 & 7 & 4 & 13 & 35 & 12 & 4 & 13 & 8 & 26 & 1 & 31 & 32 & 30 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 9 & 9 & 26 & 26 & 7 & 7 & 1 & 1 & 26 & 26 & 16 & 16 & 34 & 34 & 9 & 9 & 16 & 16 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 7 & 7 & 17 & 17 & 13 & 13 & 4 & 4 & 35 & 35 & 32 & 32 & 6 & 6 & 8 & 8 & 34 & 34 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 26 & 26 & 4 & 4 & 3 & 3 & 16 & 16 & 3 & 3 & 27 & 27 & 25 & 25 & 3 & 3 & 26 & 26 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 12 & 12 & 14 & 14 & 32 & 32 & 27 & 27 & 14 & 14 & 17 & 17 & 24 & 24 & 15 & 15 & 9 & 9 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 34 & 34 & 12 & 12 & 33 & 33 & 34 & 34 & 16 & 16 & 34 & 34 & 26 & 26 & 1 & 1 & 33 & 33 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 34 & 10 & 27 & 9 & 28 & 1 & 36 & 10 & 27 & 4 & 33 & 16 & 21 & 3 & 34 & 4 & 33 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 27 & 10 & 35 & 2 & 22 & 15 & 4 & 33 & 22 & 15 & 8 & 29 & 5 & 32 & 15 & 22 & 27 & 10 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 21 & 16 & 30 & 7 & 25 & 12 & 16 & 21 & 4 & 33 & 16 & 21 & 27 & 10 & 1 & 36 & 25 & 12
\end{pmatrix}.$$

...and as a pair of representations!

$$P_2^{-1} G Q_2 = 2 \cdot \begin{pmatrix}
8 & 11 & 1 & 6 & 10 & 23 & 1 & 6 & 1 & 6 & 8 & 11 & 10 & 23 & 8 & 11 & 8 & 11 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
35 & 25 & 22 & 21 & 8 & 11 & 4 & 24 & 17 & 28 & 16 & 22 & 17 & 28 & 3 & 18 & 17 & 28 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
19 & 3 & 3 & 18 & 36 & 31 & 16 & 22 & 30 & 32 & 32 & 7 & 3 & 18 & 15 & 16 & 13 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
23 & 27 & 29 & 26 & 14 & 10 & 27 & 14 & 29 & 26 & 27 & 14 & 31 & 1 & 1 & 6 & 23 & 27 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
15 & 21 & 26 & 29 & 34 & 18 & 1 & 31 & 26 & 29 & 2 & 25 & 33 & 24 & 15 & 21 & 2 & 25 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
24 & 4 & 17 & 9 & 5 & 7 & 4 & 13 & 35 & 12 & 4 & 13 & 8 & 26 & 1 & 31 & 32 & 30 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 9 & 9 & 26 & 26 & 7 & 7 & 1 & 1 & 26 & 26 & 16 & 16 & 34 & 34 & 9 & 9 & 16 & 16 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 7 & 7 & 17 & 17 & 13 & 13 & 4 & 4 & 35 & 35 & 32 & 32 & 6 & 6 & 8 & 8 & 34 & 34 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 26 & 26 & 4 & 4 & 3 & 3 & 16 & 16 & 3 & 3 & 27 & 27 & 25 & 25 & 3 & 3 & 26 & 26 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 12 & 12 & 14 & 14 & 32 & 32 & 27 & 27 & 14 & 14 & 17 & 17 & 24 & 24 & 15 & 15 & 9 & 9 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 34 & 34 & 12 & 12 & 33 & 33 & 34 & 34 & 16 & 16 & 34 & 34 & 26 & 26 & 1 & 1 & 33 & 33 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 34 & 10 & 27 & 9 & 28 & 1 & 36 & 10 & 27 & 4 & 33 & 16 & 21 & 3 & 34 & 4 & 33 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 27 & 10 & 35 & 2 & 22 & 15 & 4 & 33 & 22 & 15 & 8 & 29 & 5 & 32 & 15 & 22 & 27 & 10 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 21 & 16 & 30 & 7 & 25 & 12 & 16 & 21 & 4 & 33 & 16 & 21 & 27 & 10 & 1 & 36 & 25 & 12
\end{pmatrix}.$$

A Decomposition Lemma to Compute Folded Codes

Lemma [Pasquereau]

Let $G \in \mathbb{F}_q^{k\times n}$ be the generator matrix of a linear code. Suppose $LG = GR$ for some $L \in \mathrm{GL}_k(\mathbb{F}_q)$ and $R \in \mathrm{GL}_n(\mathbb{F}_q)$. If L and R are diagonalizable matrices, then there exist a pair of invertible matrices $(P, Q) \in \mathrm{GL}_k(\mathbb{F}_q) \times \mathrm{GL}_n(\mathbb{F}_q)$, such that

$$P^{-1}GQ = \begin{pmatrix} G_{i_1,j_1} & 0 & \dots & 0 \\ 0 & G_{i_2,j_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & G_{i_t,j_t} \end{pmatrix},$$

where $t = |\{\lambda_i : 1 \le i \le r\} \cap \{\mu_j : 1 \le j \le s\}|$ is the size of the intersection between the spectra of L and R, $G_{i_u,j_u} \in \mathbb{F}_q^{k_{i_u}\times n_{j_u}}$. What's more, k_{i_u} and n_{i_u} are the respective geometric dimensions of the left and right eigenspaces associated to the same eigenvalue λ_u in the intersection.
In particular there exists a family $\{Q_u\}_{1\le u\le t}$ of projections $Q_u : C \to C'_u$, where C is the code generated by G, and C'_u is an $[n_{j_u}, k_{i_u}, d_u]$-code, such that

$$\forall \mathbf{x} \in \mathbb{F}_q^n, (\mathbf{x} \in C) \iff (\forall u \in \{1, \dots, t\}, \mathbf{x}Q_u \in C'_u).$$

Recovering the FRI's folding map

$$\Phi : \begin{cases} \mathbb{F}_q^\times & \hookrightarrow & \mathrm{Aut}(\mathbb{P}^1) \\ \alpha & \mapsto & \varphi_\alpha : (x:y) \mapsto (\alpha x : y) \end{cases}$$

$$\mathsf{L} : \begin{cases} \mathrm{Aut}(\mathbb{P}^1) & \to & \mathrm{GL}(L_{\mathbb{P}^1}(D)) \cong \mathrm{GL}_k(\mathbb{F}_q) \\ \varphi & \mapsto & \varphi^* : f \mapsto f \circ \varphi \end{cases}$$

$$\mathsf{R} : \begin{cases} \mathrm{Aut}(\mathbb{P}^1) & \to & \mathrm{GL}(\mathbb{F}_q[\Gamma]) \cong \mathrm{GL}_n(\mathbb{F}_q) \\ \varphi & \mapsto & \sum_x a_{(x:1)} \mathsf{e}_{(x:1)} \mapsto \sum_x a_{(x:1)} \mathsf{e}_{\varphi(x:1)} \end{cases}$$

with D a divisor of degree $0 \leq k-1 \leq q-1$ supported by $\mathbb{F}_q^\times$-inv. points.

For a primitive element $\alpha \in \mathbb{F}_q^\times$, $\mathsf{L}(\Phi(\alpha))G = G\mathsf{R}(\Phi(\alpha))$. If k and $n = q-1$ are divisible by 2, applying the lemma to $L = \mathsf{L}(\Phi(\alpha^{\frac{q-1}{2}}))$, $R = \mathsf{R}(\Phi(\alpha^{\frac{q-1}{2}}))$, induces a folding map $\mathsf{Fold}[\mathsf{c}, z] = \mathsf{c}(Q_1 + zQ_2)$.

Conclusion: What does this framework bring?

- *Generality*: focus on generator matrices and code automorphism groups.
- *Coding Theory Techniques:* study efficiency and soundness using coding theory tools.
- *Step-by-Step Approach*: a class of code does not need to be 'closed' under folding.
- *Folding Codes* OR *Folding Structure*: free to either fix G or fix (L, R).
- *Other Metrics*: consider different classes of isometries.

- *Code Automorphism*: computing a "good" (L, R)-pair is still difficult.
- *Control of Sufficient Conditions:* less guarantees that the folded codes are balanced or have good minimal distance.
- *Code Equivalence:* can be computationally difficult to merge the projectors.

Conclusion: What does this framework bring?

- *Generality*: focus on generator matrices and code automorphism groups.
- *Coding Theory Techniques:* study efficiency and soundness using coding theory tools.
- *Step-by-Step Approach*: a class of code does not need to be 'closed' under folding.
- *Folding Codes* OR *Folding Structure*: free to either fix G or fix (L, R).
- *Other Metrics*: consider different classes of isometries.

- *Code Automorphism*: computing a "good" (L, R)-pair is still difficult.
- *Control of Sufficient Conditions:* less guarantees that the folded codes are balanced or have good minimal distance.
- *Code Equivalence:* can be computationally difficult to merge the projectors.

Thank you!

Augot, Daniel, Sarah Bordage, and Jade Nardi (Nov. 2022). “Efficient multivariate low-degree tests via interactive oracle proofs of proximity for polynomial codes”. In: *Designs, Codes and Cryptography*. DOI: 10.1007/s10623-022-01134-z.

Ben-Sasson, Eli, Iddo Bentov, et al. (2017). “Fast Reed-Solomon Interactive Oracle Proofs of Proximity”. In: *Electron. Colloquium Comput. Complex.* TR17.

Ben-Sasson, Eli, Alessandro Chiesa, and Nicholas Spooner (2016). “Interactive Oracle Proofs”. In: *Theory of Cryptography Conference*.

Ben-Sasson, Eli, Swastik Kopparty, and Shubhangi Saraf (2018). “Worst-Case to Average Case Reductions for the Distance to a Code”. In: *Electron. Colloquium Comput. Complex.* TR18.

Bordage, Sarah et al. (2020). “Interactive Oracle proofs of Proximity to Algebraic Geometry Codes”. In: *Proceedings of the 37th Computational Complexity Conference.*