$13^{th}$ AAECC Symposium
On Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes
Hawaii (USA),
November 15–19, 1999

# Quantum Reed-Solomon Codes

Markus Grassl
Willi Geiselmann & Thomas Beth

Arbeitsgruppe *Quantum Computing*
Institut für Algorithmen und Kognitive Systeme
Fakultät für Informatik, Universität Karlsruhe
Germany

# Overview

- Quantum information
- Quantum operations
- Quantum error-correcting codes (QECC)
- Construction of QECC
- Quantum Reed-Solomon codes
- Quantum implementation of linear transforms
- $\mathrm{DFT}$ over finite fields
- Concluding remarks

# Quantum Information

## Quantum-bit (qubit)

basis states:

$$\text{“0”} \mathrel{\hat{=}} |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \mathbb{C}^2, \qquad \text{“1”} \mathrel{\hat{=}} |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in \mathbb{C}^2$$

general state:

$$|q\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \text{where } \alpha, \beta \in \mathbb{C},\ |\alpha|^2 + |\beta|^2 = 1$$

## Quantum register

basis states:

$$|b_1\rangle \otimes \ldots \otimes |b_n\rangle =: |b_1 \ldots b_n\rangle = |\boldsymbol{b}\rangle \qquad \text{where } b_i \in \{0,1\}$$

general state:

$$|\psi\rangle = \sum_{\boldsymbol{x} \in \{0,1\}^n} c_{\boldsymbol{x}} |\boldsymbol{x}\rangle \qquad \text{where } \textstyle\sum_{\boldsymbol{x} \in \{0,1\}^n} |c_{\boldsymbol{x}}|^2 = 1$$

$\Longrightarrow$ normalised vector in $(\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^{2^n}$

$\Longrightarrow$ note the similarity to the group ring $\mathbb{C}[\mathbb{F}_2^n]$

# Quantum Operations: "Gates"

## $NOT$ gate

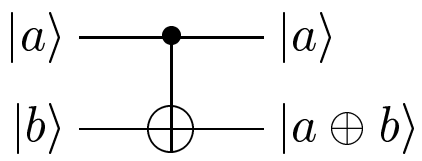
$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \begin{aligned} |0\rangle &\mapsto |1\rangle \\ |1\rangle &\mapsto |0\rangle \end{aligned}$$

## Hadamard transformation

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \begin{aligned} |0\rangle &\mapsto \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle &\mapsto \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

## Controlled $NOT$ ($CNOT$) gate

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \begin{aligned} |00\rangle &\mapsto |00\rangle \\ |01\rangle &\mapsto |01\rangle \\ |10\rangle &\mapsto |11\rangle \\ |11\rangle &\mapsto |10\rangle \end{aligned}$$



# Simple Quantum Code: Bit-Flips

$$\left.\begin{array}{rcl} |0\rangle & \mapsto & |000\rangle \\ |1\rangle & \mapsto & |111\rangle \end{array}\right\} \Longrightarrow \alpha|0\rangle + \beta|1\rangle \mapsto \alpha|000\rangle + \beta|111\rangle$$

two-dimensional subspace $\mathcal{H}_{\mathcal{C}} \leq \mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2$

| bit-flip | quantum state | subspace |
|---|---|---|
| no error | $\alpha\|000\rangle + \beta\|111\rangle$ | $(\mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1})\mathcal{H}_{\mathcal{C}}$ |
| 1st position | $\alpha\|100\rangle + \beta\|011\rangle$ | $(\sigma_x \otimes \mathbb{1} \otimes \mathbb{1})\mathcal{H}_{\mathcal{C}}$ |
| 2nd position | $\alpha\|010\rangle + \beta\|101\rangle$ | $(\mathbb{1} \otimes \sigma_x \otimes \mathbb{1})\mathcal{H}_{\mathcal{C}}$ |
| 3rd position | $\alpha\|001\rangle + \beta\|110\rangle$ | $(\mathbb{1} \otimes \mathbb{1} \otimes \sigma_x)\mathcal{H}_{\mathcal{C}}$ |

orthogonal decomposition:

$$\begin{aligned} \mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2 \quad = \quad & (\mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1})\mathcal{H}_{\mathcal{C}} \\ & \oplus (\sigma_x \otimes \mathbb{1} \otimes \mathbb{1})\mathcal{H}_{\mathcal{C}} \\ & \oplus (\mathbb{1} \otimes \sigma_x \otimes \mathbb{1})\mathcal{H}_{\mathcal{C}} \\ & \oplus (\mathbb{1} \otimes \mathbb{1} \otimes \sigma_x)\mathcal{H}_{\mathcal{C}} \end{aligned}$$

# Quantum Errors

Bit-flip:

- interchange of the basis states $|0\rangle$ and $|1\rangle$
- corresponds to "classical" bit error
- $NOT$ gate resp. $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Phase-flip:

- inversion of the *relative* phase of the states $|0\rangle$ and $|1\rangle$
- no classical analogue
- $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Combination:

- $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = i\sigma_x\sigma_z$

Conjugation:

- $H\sigma_x H = \sigma_z$
- $H\sigma_z H = \sigma_x$

} interchange of bit-flip and phase-flip

# Quantum Codes (QECC)

(Calderbank & Shor/Steane)

Definition:

Let $C = [n, k, d]$ be a weakly self-dual linear binary code, i. e., $C \leq C^{\perp}$, where $C^{\perp} = [n, n-k, d^{\perp}]$.

For coset representatives $\boldsymbol{w} \in C^{\perp}/C$, define

$$|\psi_{\boldsymbol{w}}\rangle := \frac{1}{\sqrt{|C|}} \sum_{\boldsymbol{c} \in C} |\boldsymbol{c} + \boldsymbol{w}\rangle$$

or equivalently (Hadamard transformation)

$$|\widehat{\psi}_{\boldsymbol{w}}\rangle := \frac{1}{\sqrt{|C^{\perp}|}} \sum_{\boldsymbol{c} \in C^{\perp}} (-1)^{\boldsymbol{c} \cdot \boldsymbol{w}} |\boldsymbol{c}\rangle$$

$\Longrightarrow$ quantum error-correcting code $\mathcal{C} = [[n, n-2k, d' \geq d^{\perp}]]$

Encoded quantum state:

$$|\psi\rangle = \sum_{\boldsymbol{w} \in C^{\perp}/C} \alpha_{\boldsymbol{w}} |\psi_w\rangle = \sum_{\boldsymbol{c} \in C^{\perp}} \beta_{\boldsymbol{c}} |\boldsymbol{c}\rangle$$

$$|\widehat{\psi}\rangle = \sum_{\boldsymbol{w} \in C^{\perp}/C} \widehat{\alpha}_{\boldsymbol{w}} |\widehat{\psi}_w\rangle = \sum_{\boldsymbol{c} \in C^{\perp}} \gamma_{\boldsymbol{c}} |\boldsymbol{c}\rangle$$

$\Longrightarrow$ superpositions of codewords of $C^{\perp}$

# Weakly Self-Dual Codes (I)

**Construction of QECC:**

Search for good linear binary weakly self-dual codes.

**Dual basis:**

For a basis $\mathcal{B} = (b_1, \ldots, b_\ell)$ of $\mathbb{F}_{2^\ell}|\mathbb{F}_2$ let $\mathcal{B}^\perp = (b'_1, \ldots, b'_\ell)$ denote the *dual basis* with

$$\mathrm{tr}(b_i \cdot b'_j) = \delta_{ij}.$$

**Self-dual basis:**

$$\mathcal{B} = \mathcal{B}^\perp, \text{ i. e., } \mathrm{tr}(b_i \cdot b_j) = \delta_{ij}$$

**Subfield expansion:**

For $C = [n, k, d] \leq \mathbb{F}_{2^\ell}^n$, define

$$\mathcal{B}(C) := \Big\{ (c_{11}, \ldots, c_{1\ell}, \ldots, c_{n1}, \ldots, c_{n\ell}) : \boldsymbol{c} = (c_1, \ldots, c_n) \in C,\ c_i = \textstyle\sum_{j=1}^{\ell} c_{ij} b_j \Big\}$$

$$\Longrightarrow \mathcal{B}(C) = [\ell n, \ell k, d' \geq d] \leq \mathbb{F}_2^{\ell n}$$

# Weakly Self-Dual Codes (II)

The following diagram commutes:

$$\begin{array}{ccc} C & \longrightarrow & C^{\perp} \\ \text{basis } \mathcal{B}\downarrow & & \downarrow \text{ dual basis } \mathcal{B}^{\perp} \\ \mathcal{B}(C) & \longrightarrow & \mathcal{B}^{\perp}(C^{\perp}) = (\mathcal{B}(C))^{\perp} \end{array}$$

$C = [n, k] \leq \mathbb{F}_{2^\ell}$ weakly self-dual, i. e., $C \leq C^{\perp}$,
$\mathcal{B}$ a self-dual basis of $\mathbb{F}_{2^\ell}|\mathbb{F}_2$
$\Longrightarrow \mathcal{B}(C) \leq \mathcal{B}(C^{\perp})$.

**Idea:**

- start with a weakly self-dual code $C$ over $\mathbb{F}_{2^\ell}$ and a self-dual basis $\mathcal{B}$
- obtain a weakly self-dual binary code $\mathcal{B}(C)$
- obtain a CSS code

**Advantages:**

- correction of burst errors
- suitable for concatenation
- applies to Reed-Solomon codes

# Quantum Reed-Solomon Codes

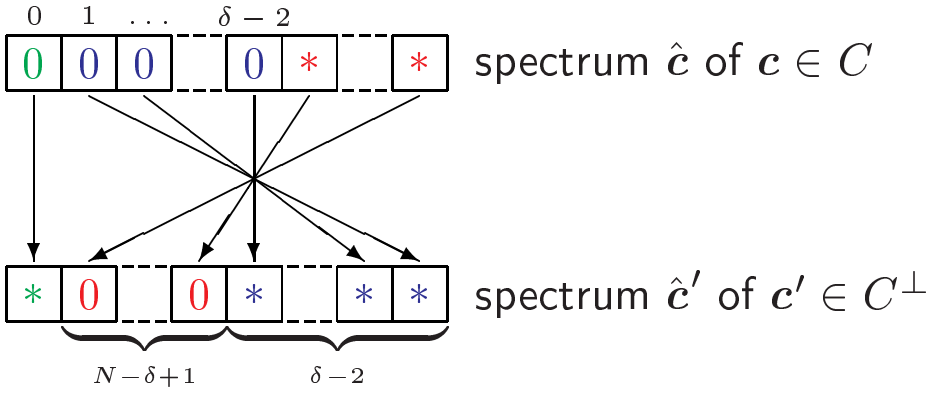
RS code $C = [n = 2^\ell - 1, n - \delta + 1, \delta]$ over $\mathbb{F}_{2^\ell}$,
generator polynomial

$$\boldsymbol{g}(X) = (X - 1)(X - \alpha) \ldots (X - \alpha^{\delta-2})$$

weakly self-dual iff $\delta > n/2 + 1$:

$$\begin{aligned}\boldsymbol{g}^\perp(X) &= (X - \alpha^{-(\delta-1)})(X - \alpha^{-\delta}) \ldots (X - \alpha^{-(n-1)}) \\ &= (X - \alpha^1)(X - \alpha^2) \ldots (X - \alpha^{n-\delta+1})\end{aligned}$$

Spectra:




Encoding & decoding:

discrete Fourier transformation over $\mathbb{F}_{2^\ell}$

$\Longrightarrow$ linear transformation over $\mathbb{F}_{2^\ell}$

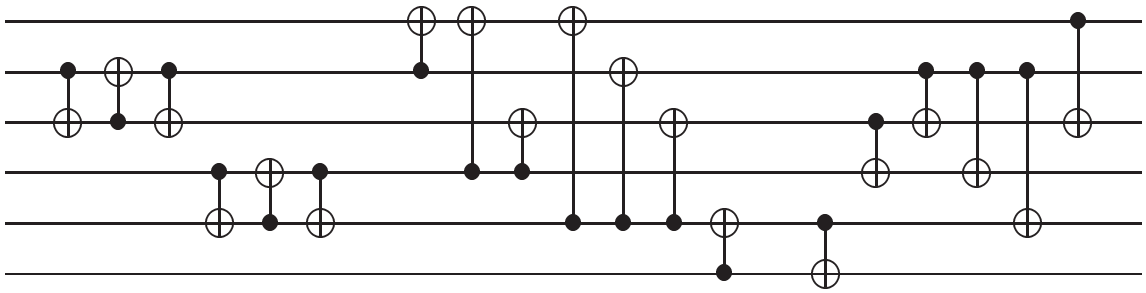
choose a basis $\mathcal{B}$ of $\mathbb{F}_{2^\ell}|\mathbb{F}_2$

$\Longrightarrow$ linear transformation over $\mathbb{F}_2$

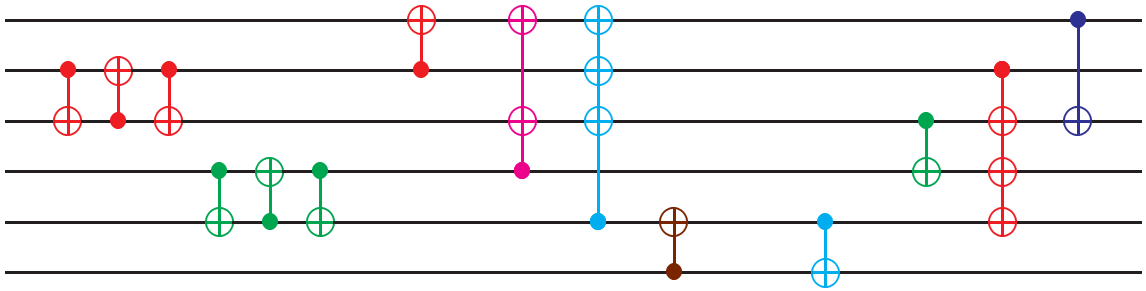
# Example: Linear Transformation over $\mathbb{F}_2$

$$\begin{pmatrix} 1 & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & 1 & \cdot & \cdot \\ 1 & 1 & \cdot & 1 & 1 & \cdot \\ 1 & 1 & 1 & \cdot & \cdot & 1 \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot \end{pmatrix} = \begin{pmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 \end{pmatrix} \begin{pmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ 1 & \cdot & 1 & 1 & \cdot & \cdot \\ 1 & 1 & 1 & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & 1 & 1 & 1 & \cdot \\ \cdot & \cdot & 1 & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 \end{pmatrix}$$

$\hat{=}$



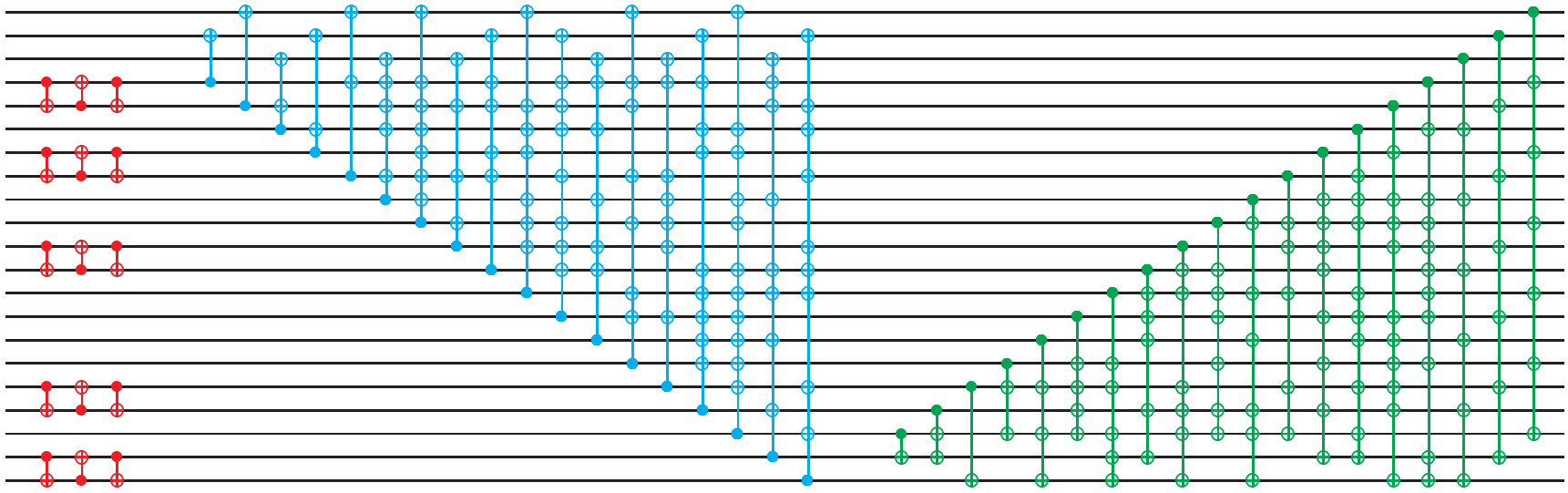
$=$



# Quantum Circuit: $\mathrm{DFT}_7$ over $\mathbb{F}_8$

$$\mathcal{B}(\mathrm{DFT}_7) := \left(\begin{array}{ccccccccccccccccccccccccccccccccccccccccccccccc}
1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot \\
\cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot \\
\cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 \\
1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & \cdot & 1 & \cdot & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 \\
\cdot & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & \cdot & 1 & 1 & \cdot & \cdot & \cdot & 1 & 1 & \cdot & \cdot & \cdot & 1 & 1 & \cdot & \cdot & \cdot & 1 & 1 & \cdot & \cdot & \cdot & 1 \\
\cdot & \cdot & 1 & \cdot & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & \cdot & \cdot \\
1 & \cdot & \cdot & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 \\
\cdot & 1 & \cdot & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & 1 & 1 & 1 & \cdot \\
\cdot & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & \cdot \\
1 & \cdot & \cdot & \cdot & 1 & \cdot & 1 & \cdot & 1 & \cdot & \cdot & 1 & \cdot & 1 & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 \\
\cdot & 1 & \cdot & 1 & \cdot & 1 & \cdot & \cdot & 1 & \cdot & 1 & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & 1 & 1 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & 1 & 1 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\
\cdot & \cdot & 1 & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 \\
1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & \cdot & 1 & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & 1 & \cdot & \cdot & 1 & 1 & \cdot & 1 & \cdot & \cdot & 1 & 1 & \cdot & 1 & \cdot & \cdot & 1 & 1 & \cdot & 1 & \cdot & \cdot \\
\cdot & 1 & \cdot & 1 & 1 & 1 & 1 & 1 & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & \cdot & 1 & \cdot \\
\cdot & \cdot & 1 & 1 & \cdot & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 \\
1 & \cdot & \cdot & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & \cdot & 1 & 1 & 1 & \cdot \\
\cdot & 1 & \cdot & \cdot & 1 & 1 & 1 & \cdot & 1 & \cdot & \cdot & 1 & \cdot & 1 & \cdot & 1 & 1 & 1 & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & 1 & 1 \\
\cdot & \cdot & 1 & 1 & 1 & \cdot & 1 & \cdot & \cdot & 1 & \cdot & 1 & 1 & 1 & 1 & \cdot & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & \cdot & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & \cdot & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & \cdot & \cdot
\end{array}\right) = \mathrm{perm} \cdot \left(\begin{array}{ccccccccccccccccccccccccccccccccccccccccccccccc}
1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & 1 & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & 1 & \cdot & \cdot & \cdot & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 & 1 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & 1 & \cdot & 1 & \cdot & 1 & \cdot & \cdot & 1 & \cdot & 1 & 1 & \cdot & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & 1 & \cdot & 1 & \cdot & 1 & 1 & \cdot & 1 & \cdot & \cdot & 1 & \cdot & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
1 & \cdot & \cdot & 1 & 1 & \cdot & 1 & 1 & \cdot & 1 & 1 & 1 & 1 & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & 1 & \cdot & 1 & 1 & \cdot & 1 & 1 & 1 & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & 1 & 1 & 1 & \cdot & 1 & \cdot & 1 & 1 & 1 & 1 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
1 & \cdot & \cdot & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & 1 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & 1 & \cdot & \cdot & \cdot & 1 & 1 & 1 & \cdot & 1 & \cdot & \cdot & 1 & \cdot & 1 & \cdot & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & 1 & 1 & 1 & \cdot & 1 & \cdot & \cdot & 1 & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
1 & \cdot & \cdot & 1 & \cdot & 1 & \cdot & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & 1 & \cdot & \cdot & 1 & 1 & 1 & \cdot & 1 & \cdot & 1 & \cdot & 1 & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & 1 & 1 & 1 & \cdot & 1 & \cdot & \cdot & 1 & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
1 & \cdot & \cdot & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & \cdot & 1 & 1 & 1 & \cdot \\
\cdot & 1 & \cdot & \cdot & 1 & 1 & 1 & \cdot & 1 & \cdot & \cdot & 1 & \cdot & 1 & \cdot & 1 & 1 & 1 & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & 1 & 1 \\
\cdot & \cdot & 1 & 1 & 1 & \cdot & 1 & \cdot & \cdot & 1 & \cdot & 1 & 1 & 1 & 1 & \cdot & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & \cdot & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & \cdot & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & \cdot & \cdot
\end{array}\right) \left(\begin{array}{ccccccccccccccccccccccccccccccccccccccccccccccc}
1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot \\
\cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot \\
\cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 \\
\cdot & \cdot & \cdot & 1 & 1 & \cdot & \cdot & \cdot & 1 & \cdot & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 \\
\cdot & \cdot & \cdot & \cdot & 1 & 1 & \cdot & \cdot & \cdot & 1 & \cdot & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & 1 & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & 1 & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & 1 & 1 & \cdot & \cdot & 1 & \cdot & 1 & 1 & 1 & \cdot & \cdot & 1 & \cdot & 1 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & 1 & \cdot & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & \cdot & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & \cdot & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & \cdot & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & 1 & 1 & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & 1 & 1 & 1 & 1 & 1 & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & \cdot & 1 & 1 & 1 & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & 1 & 1 & \cdot & 1 & 1 & \cdot & 1 & 1 & \cdot & 1 & 1 & \cdot & 1 & 1 & \cdot & 1 & 1 & \cdot & 1 & 1 & \cdot & 1 & 1 & \cdot & 1 & 1 & \cdot & 1 & 1 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & \cdot & \cdot & 1 & 1 & 1 & 1 & \cdot & \cdot & 1 & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & 1 & \cdot & \cdot & 1 & \cdot & 1 & 1 & \cdot & \cdot & 1 & \cdot & 1 & 1 & \cdot & \cdot & 1 & \cdot & 1 & 1 & \cdot & \cdot & 1 & \cdot & 1 & 1 & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 & 1 & 1 & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & 1 & 1 & 1 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot & \cdot & 1 & 1 & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1
\end{array}\right)$$

$\hat{=}$



# Conclusion & Outlook

- new method to construct QECC
- also applicable for BCH codes (see quant-ph/9910060)
- correction of burst errors
- decoding either as codes over $\mathbb{F}_{2^\ell}$ or $\mathbb{F}_2$
- a lot of encoding/decoding techniques exist, e. g., using quantum linear shift registers (see quant-ph/9910061)

Further references:

http://iaks-www.ira.uka.de/home/grassl/

http://iaks-www.ira.uka.de/QIV/

and a lot of preprints at

http://xxx.lanl.gov/archive/quant-ph/