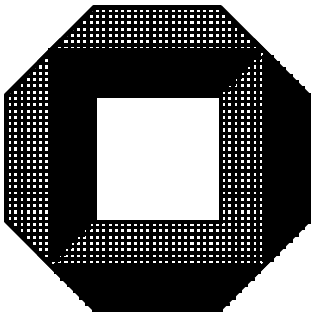
Dagstuhl Seminar

Quantum Algorithms

Algorithms for Encoding and Decoding Quantum Error–Correcting Codes

Markus Grassl

Thomas Beth



Institut für Algorithmen und Kognitive Systeme

Universität Karlsruhe

Germany

Outline

- Encoding/Decoding System (Overview)
- "Binary" Codes (Steane; Shor & Calderbank)
  - Encoding
  - Syndrome Computation
- Stabilizer/$GF(4)$–Codes (Gottesman; Calderbank, Rains, Shor & Sloane)
  - Naive Encoding
  - Efficient Encoding (Cleve & Gottesman)
  - Syndrome Computation
- Cyclic Codes
  - Some Properties
  - Error Correction
- Concluding Remarks

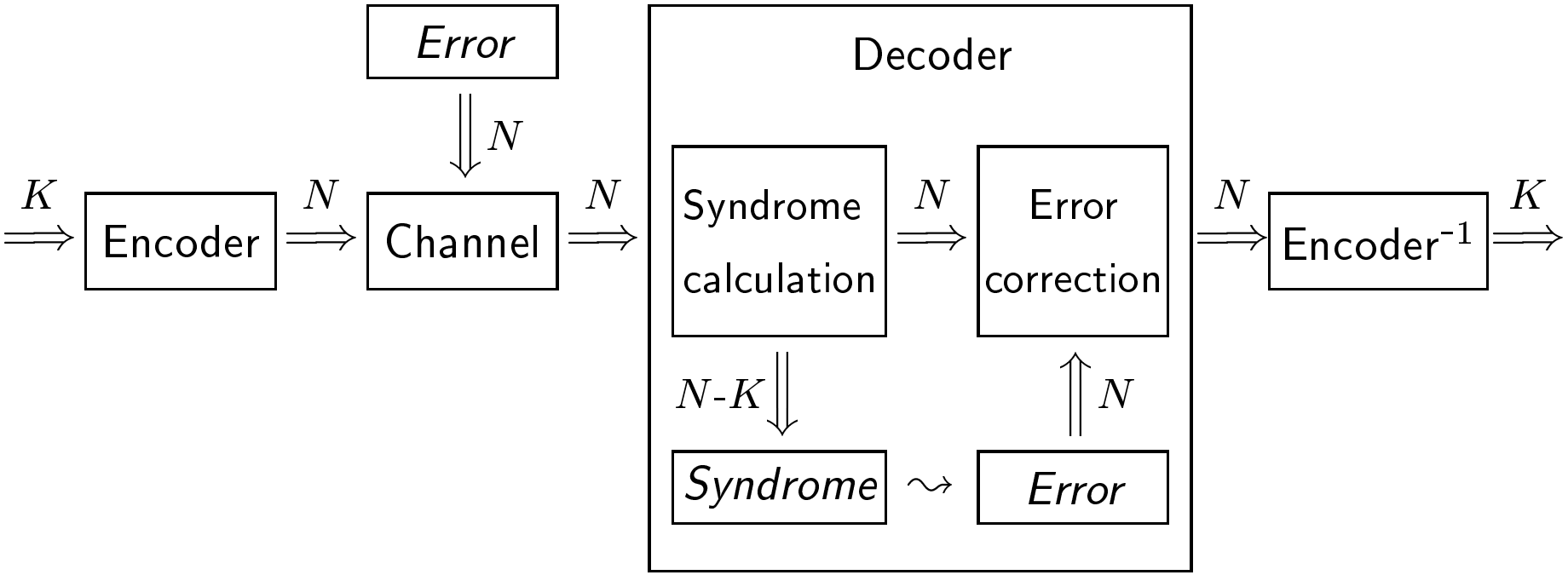
Related Literature

Richard Cleve and Daniel Gottesman.
"Efficient computations of encodings
for quantum error correction."
Physical Review A, vol. 56, no. 1, pp. 76–82 (1997).
LANL preprint quant-ph/9607030.

Markus Grassl and Thomas Beth.
"Codierung und Decodierung zyklischer
Quantencodes."
Proceedings *Fachtagung Informations– und
Mikrosystemtechnik*, Magdeburg, 25.–27.3.1998,
pp. 137–144.

Thomas Beth and Markus Grassl.
"The Quantum Hamming and Hexacodes."
To appear in *Fortschritte der Physik*, vol. 46, no. 4/5
(1998).

System Overview



Encoding and decoding using an $[[N, K]]$ quantum error–correcting code.

Linear Codes

vector spaces:	$\mathcal{C} \leq \mathbb{F}^N$
generating matrix:	$G \in \mathbb{F}^{K \times N}$
encoding:	$\boldsymbol{c} = \boldsymbol{i} \cdot G$
parity check matrix:	H^t, $G \cdot H^t = 0$
syndrome:	$\boldsymbol{s} = \boldsymbol{r} \cdot H^t$
decoding:	in general hard to decode

Encoding "Binary" Codes (I)

(Steane; Calderbank & Shor)

Given a binary code $\mathcal{C}$ with $\mathcal{C} \leq \mathcal{C}^{\perp}$, e. g.,

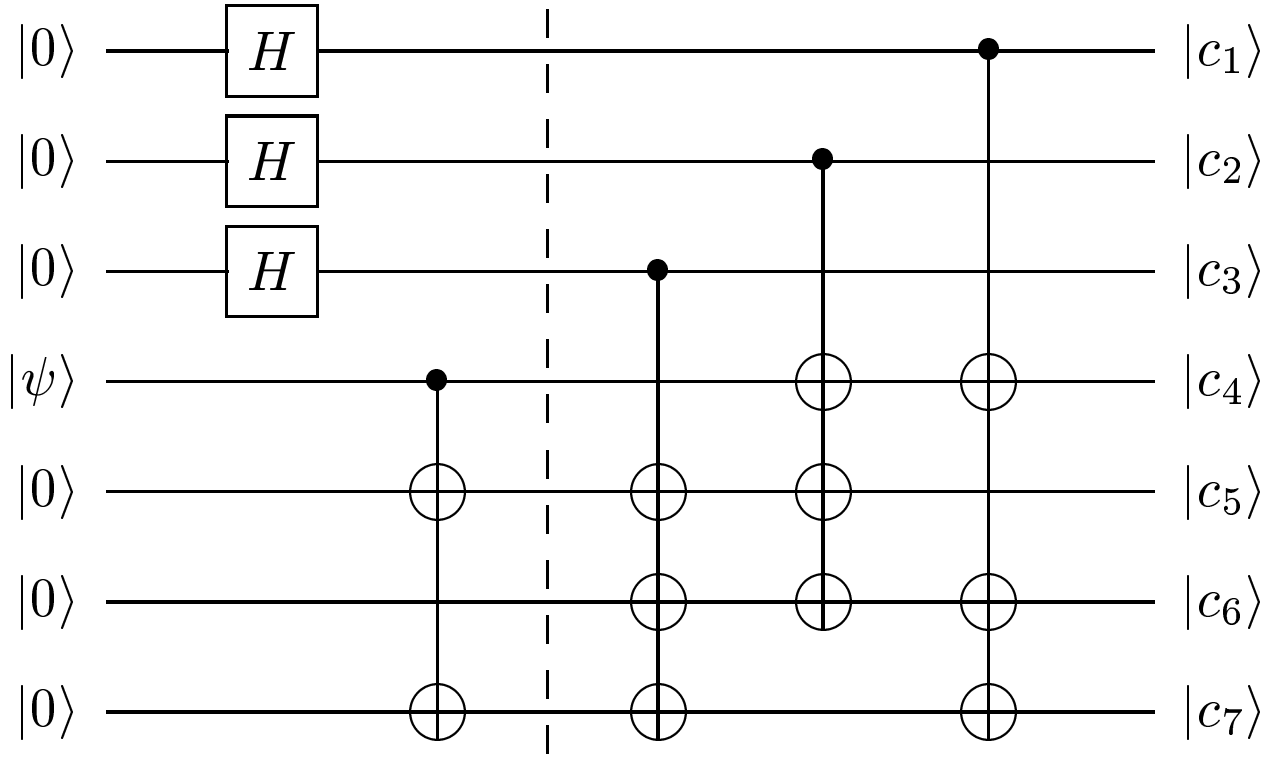
$$G = \left(\begin{array}{ccccccc} 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ \hline 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right),$$

the encoded states are:

$$|\psi_i\rangle = \frac{1}{\sqrt{|\mathcal{C}|}} \sum_{\boldsymbol{c}\in\mathcal{C}} |\boldsymbol{c} + \boldsymbol{w}_i\rangle \qquad \text{where } \boldsymbol{w}_i \in \mathcal{C}^{\perp}/\mathcal{C}.$$

Encoding "Binary" Codes (II)

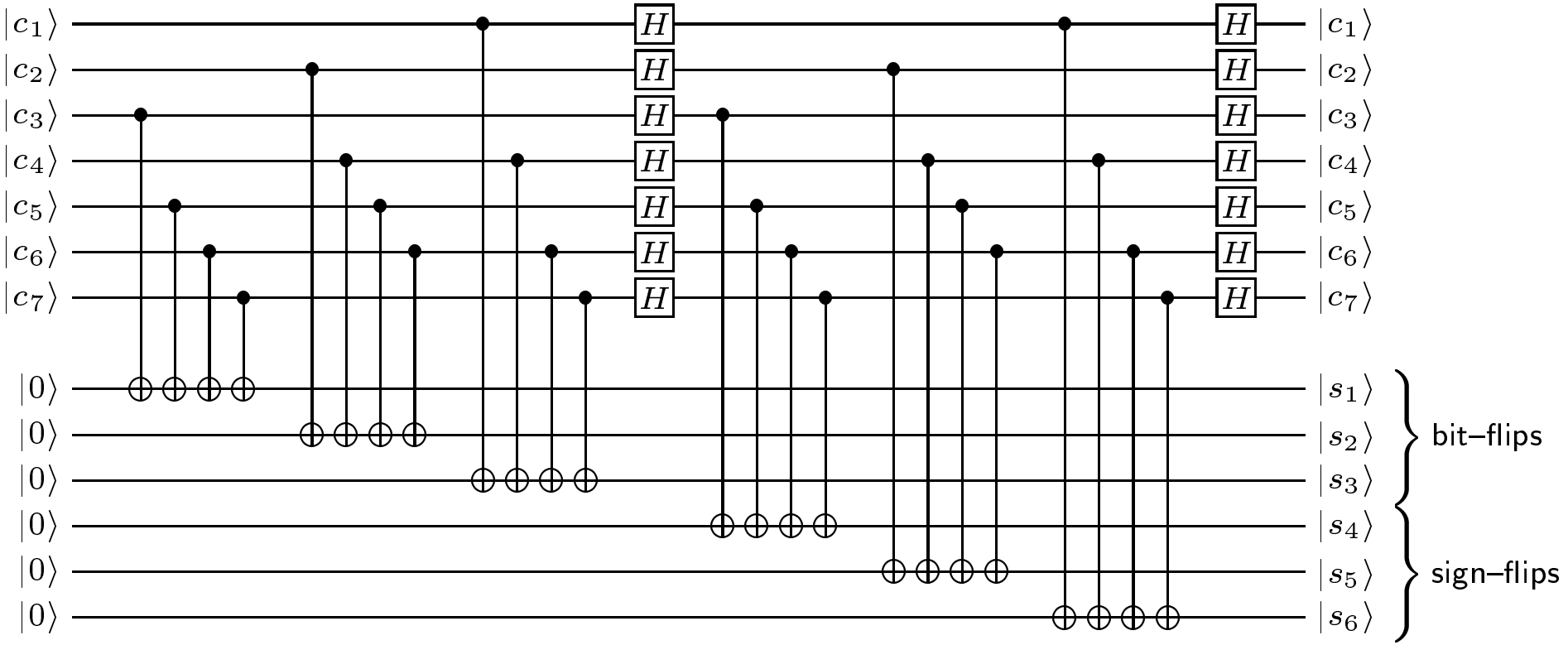
$$G^t = \left(\begin{array}{c|ccc} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{array}\right)$$



Syndrome of "Binary" Codes

$$H^t = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

$$|\psi_i\rangle = \frac{1}{\sqrt{|\mathcal{C}|}} \sum_{\boldsymbol{c}\in\mathcal{C}} |\boldsymbol{c}+\boldsymbol{w}_i\rangle \qquad H^{\otimes N}\,|\psi_i\rangle = \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{\boldsymbol{c}\in\mathcal{C}^\perp} (-1)^{\boldsymbol{c}\cdot\boldsymbol{w}_i}\,|\boldsymbol{c}\rangle$$



Encoding Stabilizer Codes (I)

$GF(4)$–Code	Pauli matrices
$G = \begin{pmatrix} 1 & 0 & 1 & \overline{\omega} & \overline{\omega} \\ \omega & 0 & \omega & 1 & 1 \\ 0 & 1 & \overline{\omega} & \overline{\omega} & 1 \\ 0 & \omega & 1 & 1 & \omega \end{pmatrix} = \begin{pmatrix} \boldsymbol{g}_1 \\ \boldsymbol{g}_2 \\ \boldsymbol{g}_3 \\ \boldsymbol{g}_4 \end{pmatrix}$	$g_1 = \sigma_x \otimes id \otimes \sigma_x \otimes \sigma_y \otimes \sigma_y$ $g_2 = \sigma_z \otimes id \otimes \sigma_z \otimes \sigma_x \otimes \sigma_x$ $g_3 = id \otimes \sigma_x \otimes \sigma_y \otimes \sigma_y \otimes \sigma_x$ $g_4 = id \otimes \sigma_z \otimes \sigma_x \otimes \sigma_x \otimes \sigma_z$

Stabilizer group: $\mathcal{S} = \langle g_1, g_2, g_3, g_4 \rangle$

Encoded state:

Sum of the orbit of the initial state $|\phi_i\rangle$ under the stabilizer group:

$$|\psi_i\rangle = \frac{1}{\sqrt{|\mathcal{S}|}} \sum_{g \in \mathcal{S}} g\,|\phi_i\rangle = \frac{1}{\sqrt{2^s}} \sum_{\boldsymbol{j} \in \mathbb{F}_2^s} g_1^{j_1} \cdot \ldots \cdot g_s^{j_s}\,|\phi_i\rangle$$

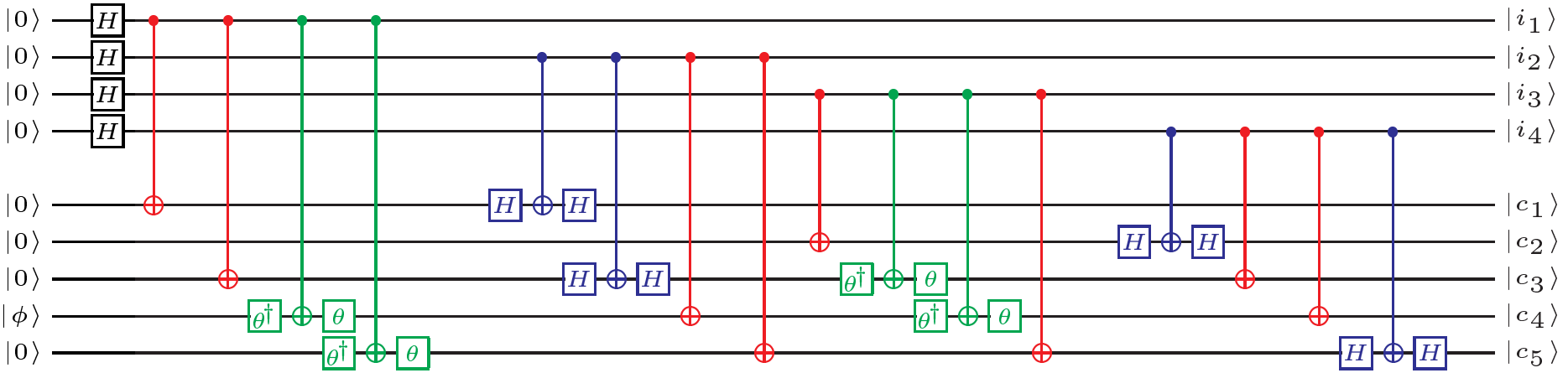
Encoding Stabilizer Codes (II)

$g_1 = (1, 0, 1, \overline{\omega}, \overline{\omega}) \mathrel{\hat{=}} \sigma_x \otimes id \otimes \sigma_x \otimes \sigma_y \otimes \sigma_y$

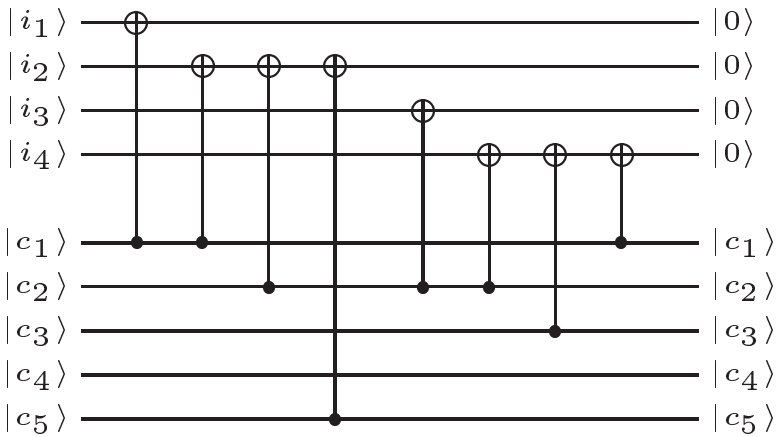
$g_2 = (\omega, 0, \omega, 1, 1) \mathrel{\hat{=}} \sigma_z \otimes id \otimes \sigma_z \otimes \sigma_x \otimes \sigma_x$

$g_3 = (0, 1, \overline{\omega}, \overline{\omega}, 1) \mathrel{\hat{=}} id \otimes \sigma_x \otimes \sigma_y \otimes \sigma_y \otimes \sigma_x$

$g_4 = (0, \omega, 1, 1, \omega) \mathrel{\hat{=}} id \otimes \sigma_z \otimes \sigma_x \otimes \sigma_x \otimes \sigma_z$



Computation of the sum of the orbit under the stabilizer group, followed by dis–entangling the 4 auxiliary qubits.



Encoding Stabilizer Codes (III)

Better: efficient encoding of Cleve & Gottesman

Standard form of the generators/generating matrix:

$$G = \begin{pmatrix} 1 & 0 & 1 & \overline{\omega} & \overline{\omega} \\ \omega & 0 & \omega & 1 & 1 \\ 0 & 1 & \overline{\omega} & \overline{\omega} & 1 \\ 0 & \omega & 1 & 1 & \omega \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 1 & \omega & 0 & \omega \\ 1+\omega & 0 & 1+\omega & \omega & \omega \\ 1+\omega & \omega & \omega & 1+\omega & 0 \\ 1 & \omega & 0 & \omega & 1 \end{pmatrix}$$

Encoded states:

$$|\psi_i\rangle = \frac{1}{\sqrt{2^4}}(\mathbb{1}+g_4)(\mathbb{1}+g_3)(\mathbb{1}+g_2)(\mathbb{1}+g_1)\Big(|i\rangle\,|0000\rangle\Big)$$

Encoding Stabilizer Codes (IV)

Basic idea:

$$\frac{1}{\sqrt{2}}(\mathbb{1}+\sigma_x)=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&1\end{pmatrix}$$

is not unitary, but

$$\begin{aligned}\frac{1}{\sqrt{2}}(\mathbb{1}+\sigma_x)\,|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\\ &= \frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}|0\rangle = H\,|0\rangle\,.\end{aligned}$$

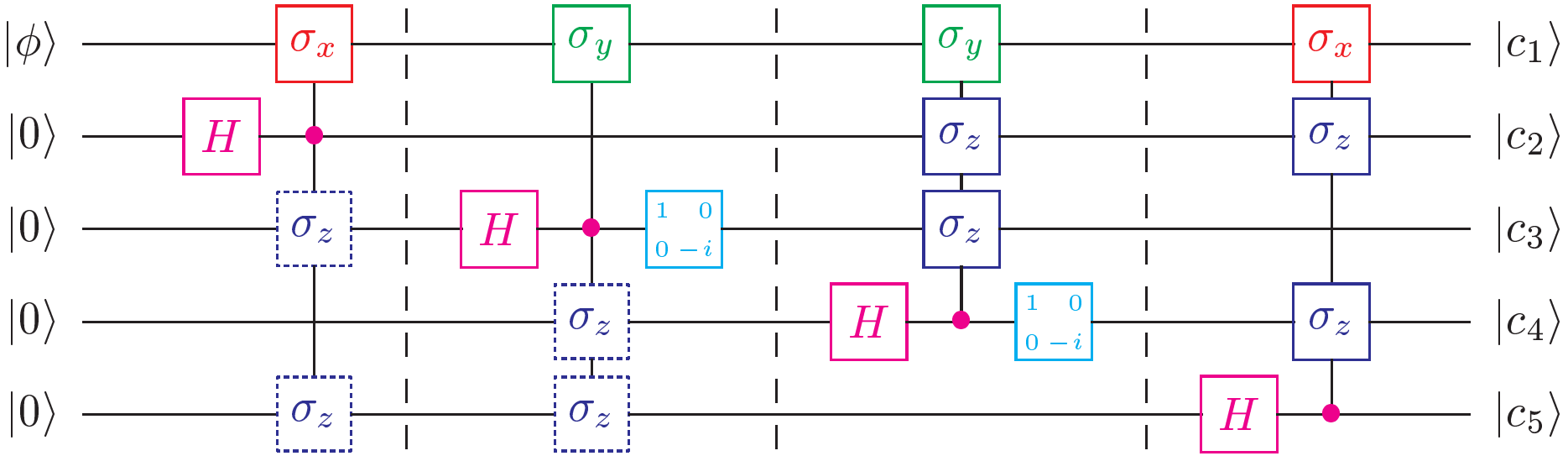
Hence:

$$\begin{aligned}&\frac{1}{\sqrt{2}}\Big(\mathbb{1}+(\sigma_x\otimes\tilde{g})\Big)\Big(|0\rangle\otimes|\varphi\rangle\Big)\\ &\quad=\frac{1}{\sqrt{2}}\Big(|0\rangle\otimes|\varphi\rangle+|1\rangle\otimes\tilde{g}\,|\varphi\rangle\Big)\\ &\quad=\Big(|0\rangle\langle 0|\otimes\mathbb{1}+|1\rangle\langle 1|\otimes\tilde{g}\Big)\big(H\otimes\mathbb{1}\big)\big(|0\rangle\otimes|\varphi\rangle\big).\end{aligned}$$

Similar for $\mathbb{1}+(\sigma_y\otimes\tilde{g})$:
$1/\sqrt{2}(\mathbb{1}+\sigma_y)\,|0\rangle=\mathrm{diag}(1,-i)H\,|0\rangle$

Encoding Stabilizer Codes ($\mathbb{V}$)

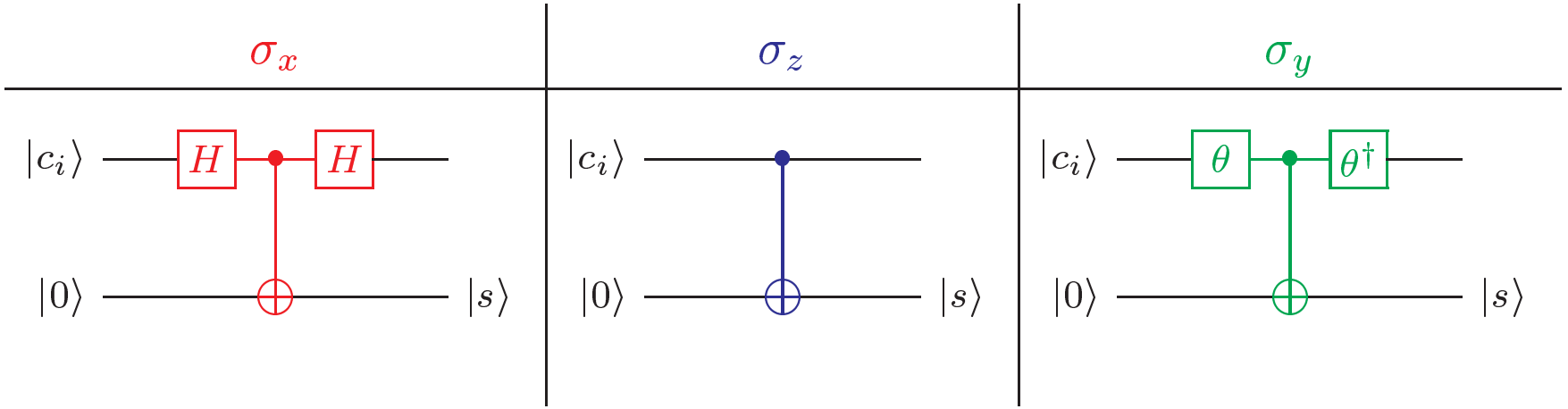
$$G^t = \begin{pmatrix} 1 & 1+\omega & 1+\omega & 1 \\ 1 & 0 & \omega & \omega \\ \omega & 1+\omega & \omega & 0 \\ 0 & \omega & 1+\omega & \omega \\ \omega & \omega & 0 & 1 \end{pmatrix}$$



Decoding Stabilizer Codes (I)

Computation of the syndrome:

Non–demolition measurement of the eigenvalues of the generators of the stabilizer group



Decoding Stabilizer Codes (II)

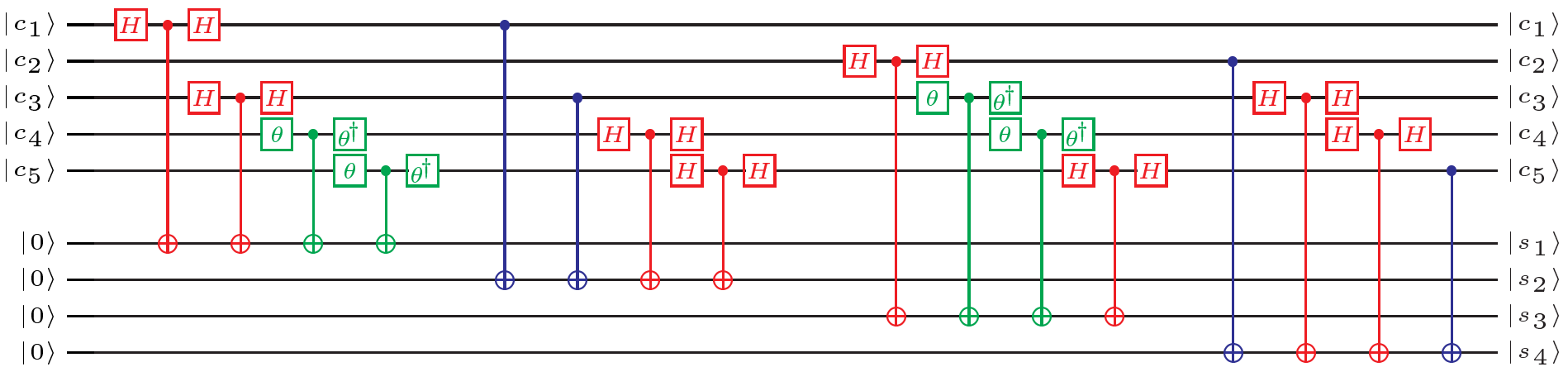
Computation of the syndrome

$g_1 = (1, 0, 1, \overline{\omega}, \overline{\omega}) \mathrel{\hat{=}} \sigma_x \otimes id \otimes \sigma_x \otimes \sigma_y \otimes \sigma_y$

$g_2 = (\omega, 0, \omega, 1, 1) \mathrel{\hat{=}} \sigma_z \otimes id \otimes \sigma_z \otimes \sigma_x \otimes \sigma_x$

$g_3 = (0, 1, \overline{\omega}, \overline{\omega}, 1) \mathrel{\hat{=}} id \otimes \sigma_x \otimes \sigma_y \otimes \sigma_y \otimes \sigma_x$

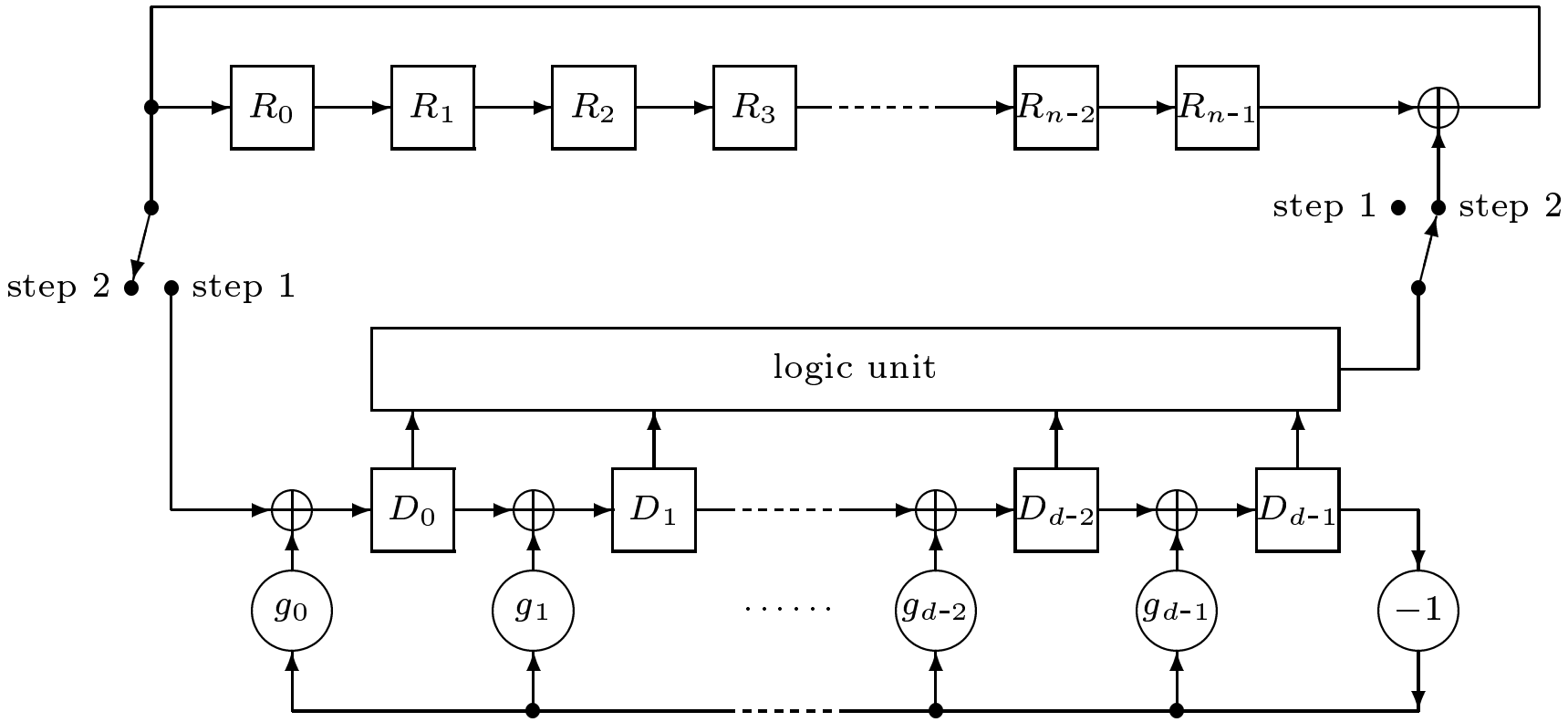
$g_4 = (0, \omega, 1, 1, \omega) \mathrel{\hat{=}} id \otimes \sigma_z \otimes \sigma_x \otimes \sigma_x \otimes \sigma_z$



Cyclic Codes (I)

Linear Codes	Cyclic Linear Codes
vector spaces $\mathcal{C} \leq \mathbb{F}^N$	polynomial ideals $\mathcal{C} \trianglelefteq \mathbb{F}[X]/(X^N - 1)$
generating matrix $G \in \mathbb{F}^{K \times N}$	generating polynomial $g(X) \mid X^N - 1$ of degree $N - K$
encoding: $\boldsymbol{c} = \boldsymbol{i} \cdot G$	encoding: $c(X) = i(X) \cdot g(X) \bmod (X^N - 1)$
parity check matrix H^t	check polynomial $g(X)$
syndrome: $\boldsymbol{s} = \boldsymbol{r} \cdot H^t$	syndrome: $s(X) = r(X) \bmod g(X)$
in general hard to decode	some efficient decoding algorithms cyclic shifting the code corresponds to shifting the syndrome $\bmod g(X)$

Meggitt–Decoder



Error correction circuit based on the Meggitt–decoder.

Cyclic Codes (II)

Correction of the error for cyclic codes