Stabilizer quantum codes via the CWS framework

Leonid Pryadko
University of California, Riverside

Y. Li, I. Dumer, & LPP, PRL (2010)
Y. Li, I. Dumer, M. Grassl, & LPP, PRA (2010)
A. Kovalev, I. Dumer, & LPP, PRA (accepted)

NSF ARO

Stabilizer quantum codes via the CWS framework

Leonid Pryadko
University of California, Riverside

- Intro: Stabilizer codes, graph states, and CWS codes
- Upper bounds on generic CWS codes
- GF(4) representation of an additive CWS code & lower bound for codes from a given graph
- Cyclic CWS & related codes

Y. Li, I. Dumer, & LPP, PRL (2010)
Y. Li, I. Dumer, M. Grassl, & LPP, PRA (2010)
A. Kovalev, I. Dumer, & LPP, PRA (accepted)

NSF ARO

Stabilizer codes

General quantum code is a subspace $\mathcal{Q}$ of n-qubit Hilbert space $\mathcal{H}_2^{\otimes n}$.

Stabilizer code $\mathcal{Q}$ is determined by an Abelian *stabilizer group* $\mathscr{S}$ of Pauli operators

$$\mathcal{Q} \equiv \{|\psi\rangle : S\,|\psi\rangle = |\psi\rangle\,, \forall S \in \mathscr{S}\}$$

If $\mathscr{S} = \langle G_1, \ldots, G_{n-k}\rangle$, with $(n-k)$ generators, the code encodes k logical qubits. There are k logical operators $\overline{X}_i$, $\overline{Z}_i$, $i = 1, \ldots, k$ which commute with every element in $\mathscr{S}$. The code is denoted $[[n, k, d]]$, where d is the distance of the code.

Errors are detected by measuring the generators G_i of the stabilizer $\mathscr{S}$

The group $\langle G_1, \ldots, G_{n-k}, Z_1, \ldots, Z_k\rangle$ stabilizes a unique stabilizer state $|s\rangle \equiv |\bar{0}\ldots\bar{0}\rangle$; the basis of the code is $|\alpha_1, \ldots \alpha_k\rangle \equiv \overline{X}_1^{\alpha_1} \ldots \overline{X}_k^{\alpha_k}\,|s\rangle$, $\alpha_j = \{0, 1\}$, $j = 1, \ldots, k$.

Example: [[5,1,3]] stabilizer code

$\mathcal{Q} \equiv \{|\psi\rangle : G_i |\psi\rangle = |\psi\rangle, i = 1, \ldots, 4\}$ with generators
$G_1 = XZZXI$, $G_2 = IXZZX$, $G_3 = XIXZZ$, $G_4 = ZXIXZ$
A basis of the code space is (up to normalization)

$$|\bar{0}\rangle = \prod_{i=1}^{4}(\mathbf{1} + G_i)|00000\rangle, \quad |\bar{1}\rangle = \overline{X}|\bar{0}\rangle.$$

The logical operators can be taken as

$$\overline{X} = ZZZZZ, \quad \overline{Z} = XXXXX.$$

Measure generators of the stabilizer to find the error, e.g.,
$\left|\tilde{\psi}\right\rangle = X_1(A|\bar{0}\rangle + B|\bar{1}\rangle)$ gives unique syndrome

$$\langle G_1\rangle = 1,\ \langle G_2\rangle = 1,\ \langle G_3\rangle = 1,\ \langle G_4\rangle = -1.$$

For this code, there are total of 15 single-qubit errors, and exactly 15 distinct syndromes (apart from $\langle G_i\rangle = 1$ for any $|\psi\rangle \in \mathcal{Q}$).

Graph states

For a simple graph $\mathcal{G} = (V, E)$ with adjacency matrix $R \equiv \gamma_{ij}$,

the generators $S_i \equiv X_i \prod_{j=1}^{n} Z^{\gamma_{ij}}$

These define the Abelian graph stabilizer group $\mathscr{S}_{\mathcal{G}} \equiv \langle S_1, \ldots, S_n \rangle$ and the graph state $|s\rangle$: $S_i |s\rangle = |s\rangle$, a $[[n, 0, d]]$ stabilizer code

Distance of a graph state is defined as the minimum weight of an element of the graph stabilizer $\mathscr{S}_{\mathcal{G}}$.

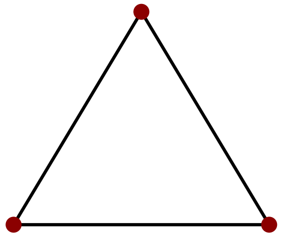
Graph states

For a simple graph $\mathcal{G} = (V, E)$ with adjacency matrix $R \equiv \gamma_{ij}$,

the generators $S_i \equiv X_i \prod_{j=1}^{n} Z^{\gamma_{ij}}$

These define the Abelian graph stabilizer group $\mathscr{S}_{\mathcal{G}} \equiv \langle S_1, \ldots, S_n \rangle$ and the graph state $|s\rangle$: $S_i |s\rangle = |s\rangle$, a $[[n, 0, d]]$ stabilizer code

Distance of a graph state is defined as the minimum weight of an element of the graph stabilizer $\mathscr{S}_{\mathcal{G}}$.



Example: Ring graph for $n = 3$; $S_1 = XZZ$, $S_2 = ZXZ$, $S_3 = ZZX$. $|s\rangle$ is an equal superposition of all 2^3 states, taken with positive or negative signs depending on the number of pairs of ones at positions connected by the edges of the graph.

$$|s\rangle = |000\rangle + |001\rangle + |010\rangle - |011\rangle + |100\rangle - |101\rangle - |110\rangle - |111\rangle$$
$$= S_2|s\rangle = |010\rangle - |011\rangle + |000\rangle + |001\rangle - |110\rangle - |111\rangle + |100\rangle - |101\rangle$$

Code-Word Stabilized codes

Invented by Cross, Smith, Smolin & Zeng (2007).

Generally non-additive, but include all stabilizer codes as a subclass.

Standard form: $\mathcal{Q} = (\mathcal{G}, \mathcal{C})$. Graph $\mathcal{G} \to$ graph state $|s\rangle$
Classical binary code $(n, K, d) = \mathcal{C} = \{\mathbf{c}_i\}_{i=1}^{K}$, with n-bit $\mathbf{c}_i$.
Quantum basis vectors $|i\rangle \equiv W_i\,|s\rangle$
codeword operators $W_i \equiv Z^{c_{i,1}} \ldots Z^{c_{i,n}}$.

Error $E = Z^{\mathbf{u}} X^{\mathbf{v}}$ maps to binary vector $[\mathrm{Cl}_{\mathcal{G}}(E)]_j \equiv u_j + \gamma_{ij} v_i$

Example: Non-additive CWS code $((5, 6, 2))$. The $n = 5$ ring graph generated by $S_2 = ZXZII$ and cyclic permutations.
Classical codewords
$c_0 = 00000$, $c_1 = 01101$, $c_2 = 10110$,
$c_3 = 01011$, $c_4 = 10101$, $c_5 = 11010$.

Code-Word Stabilized codes

Invented by Cross, Smith, Smolin & Zeng (2007).

Generally non-additive, but include all stabilizer codes as a subclass.

Standard form: $\mathcal{Q} = (\mathcal{G}, \mathcal{C})$. Graph $\mathcal{G} \to$ graph state $|s\rangle$
Classical binary code $(n, K, d) = \mathcal{C} = \{\mathbf{c}_i\}_{i=1}^{K}$, with n-bit $\mathbf{c}_i$.
Quantum basis vectors $|i\rangle \equiv W_i\,|s\rangle$
codeword operators $W_i \equiv Z^{c_{i,1}} \ldots Z^{c_{i,n}}$.

Error $E = Z^{\mathbf{u}} X^{\mathbf{v}}$ maps to binary vector $[\mathrm{Cl}_{\mathcal{G}}(E)]_j \equiv u_j + \gamma_{ij} v_i$

Example: Non-additive CWS code $((5, 6, 2))$. The $n = 5$ ring graph generated by $S_2 = ZXZII$ and cyclic permutations.
Classical codewords
$c_0 = 00000$, $c_1 = 01101$, $c_2 = 10110$,
$c_3 = 01011$, $c_4 = 10101$, $c_5 = 11010$.

Unfortunately, no known efficient algorithm to decode non-additive CWS codes.

Error correction for CWS codes

Error detection condition $\langle i| E |j\rangle = C_E \delta_{ij}$
(a) Non-degenerate case $C_E = 0$:
$0 = \langle i| E |j\rangle = \langle s| W_i^\dagger E W_j S |s\rangle = \pm \langle s| W_i^\dagger W_j (ES) |s\rangle$.
If $E = X^{\mathbf{v}} Z^{\mathbf{u}}$, get rid of all X operators with S_i: $v_i \neq 0$

Error mapping to binary vector $[\mathrm{Cl}_{\mathcal{G}}(E)]_j \equiv u_j + \gamma_{ij} v_i$

Power of Z: $c_i \oplus c_j \oplus \mathrm{Cl}_{\mathcal{G}}(E)$
If this is non-zero, classical and quantum error detection conditions coinside

(b) Degenerate case $C_E \neq 0$. Nothing to do in classical case.
Quantum: E must commute with every $W_i \Rightarrow \langle \mathbf{c}_i, \mathbf{v}\rangle = 0$

Upper bounds for a CWS code

- Distance of a CWS code $\mathcal{Q} = (\mathcal{G}, \mathcal{C})$ does not exceed that of the binary code $\mathcal{C}$, $d_{\mathcal{Q}} \le d_{\mathcal{C}}$.
- Distance of a non-degenerate CWS code $\mathcal{Q} = (\mathcal{G}, \mathcal{C})$ does not exceed that of the graph state induced by $\mathcal{G}$ [Grassl et al., 2009], $d_{\mathcal{Q}}^{\mathrm{non-deg}} \le d'_{\mathcal{G}}$
- If a bit j is involved in the code $\mathcal{C}$ $[\exists \mathbf{c} \in \mathcal{C} : \mathbf{c}_j \neq 0]$, then the distance of the CWS code $\mathcal{Q} = (\mathcal{G}, \mathcal{C})$ does not exceed the weight of S_j, $d_{\mathcal{Q}} \le \mathrm{wgt}\, S_j$.

Upper bounds for a CWS code

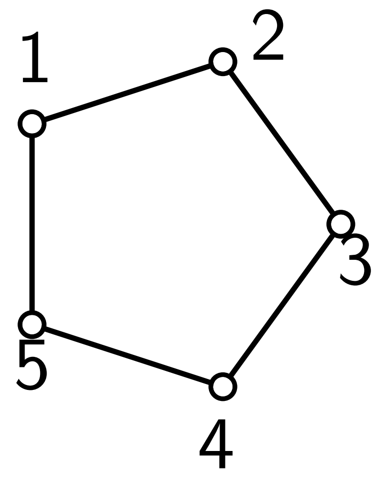
- Distance of a CWS code $\mathcal{Q} = (\mathcal{G}, \mathcal{C})$ does not exceed that of the binary code $\mathcal{C}$, $d_\mathcal{Q} \leq d_\mathcal{C}$.
- Distance of a non-degenerate CWS code $\mathcal{Q} = (\mathcal{G}, \mathcal{C})$ does not exceed that of the graph state induced by $\mathcal{G}$ [Grassl et al., 2009], $d_\mathcal{Q}^{\text{non-deg}} \leq d'_\mathcal{G}$
- If a bit j is involved in the code $\mathcal{C}$ $[\exists \mathbf{c} \in \mathcal{C} : \mathbf{c}_j \neq 0]$, then the distance of the CWS code $\mathcal{Q} = (\mathcal{G}, \mathcal{C})$ does not exceed the weight of S_j, $d_\mathcal{Q} \leq \operatorname{wgt} S_j$.

Consequences

- For a graph $\mathcal{G}$ with all vertices of the same degree r, the distance of a CWS code $\mathcal{Q} = (\mathcal{G}, \mathcal{C})$ cannot exceed $r + 1$.
- The distance of a CWS code $\mathcal{Q} = (\mathcal{G}, \mathcal{C})$ where the binary code $\mathcal{C}$ involves all bits cannot be bigger than the *minimum* weight of S_i.

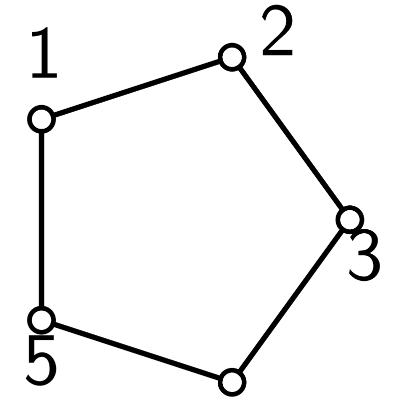
Examples: Simple stabilizer codes via CWS framework

- The $[[5, 1, 3]]$ code is generated by the binary code $\mathcal{C} = \langle(11111)\rangle$ and the 5-ring graph $\mathcal{G}$. Graph stabilizer generators $S_2 = Z_1X_2Z_3$ and cyclic shifts. Stabilizer generators $S_2S_3 = Z_1Y_2Y_3Z_4$ and cyclic shifts.

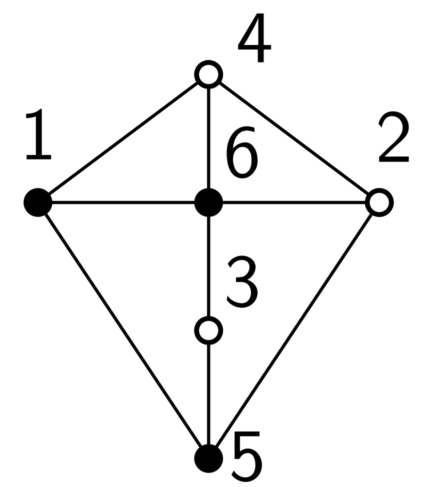


Examples: Simple stabilizer codes via CWS framework

- The $[[5,1,3]]$ code is generated by the binary code $\mathcal{C} = \langle(11111)\rangle$ and the 5-ring graph $\mathcal{G}$. Graph stabilizer generators $S_2 = Z_1X_2Z_3$ and cyclic shifts. Stabilizer generators $S_2S_3 = Z_1Y_2Y_3Z_4$ and cyclic shifts.

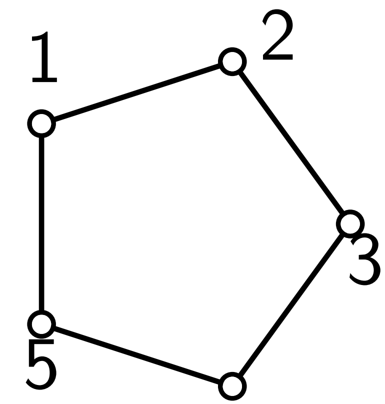


- The second $[[6,1,3]]$ code is generated by the binary code $\mathcal{C} = \langle(011100)\rangle$ and the graph shown. Code degenerate above the graph distance $d'(\mathcal{G}) = 2$: $S_1S_2 = X_1X_2$.

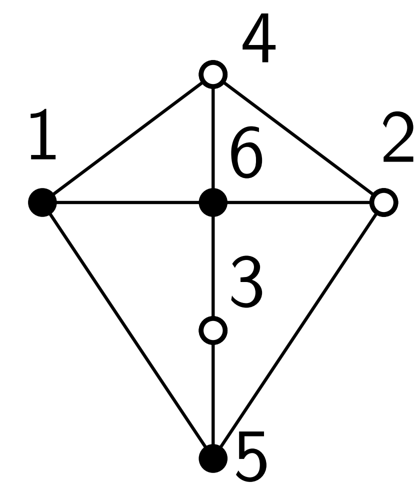


Examples: Simple stabilizer codes via CWS framework

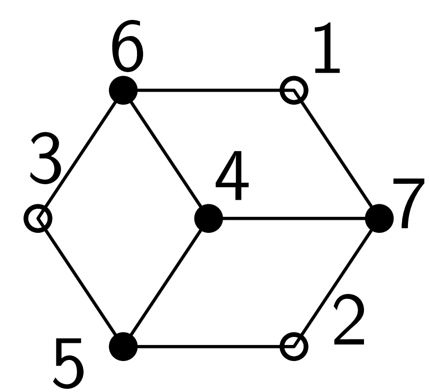
- The $[[5,1,3]]$ code is generated by the binary code $\mathcal{C} = \langle(11111)\rangle$ and the 5-ring graph $\mathcal{G}$. Graph stabilizer generators $S_2 = Z_1 X_2 Z_3$ and cyclic shifts. Stabilizer generators $S_2 S_3 = Z_1 Y_2 Y_3 Z_4$ and cyclic shifts.



- The second $[[6,1,3]]$ code is generated by the binary code $\mathcal{C} = \langle(011100)\rangle$ and the graph shown. Code degenerate above the graph distance $d'(\mathcal{G}) = 2$: $S_1 S_2 = X_1 X_2$.



- Steane's $[[7,1,3]]$ code with the stabilizer generators $X_1 X_2 X_3 X_4$, $Z_1 Z_2 Z_3 Z_4$ and their cyclic shifts. It is generated by the code $\mathcal{C} = \langle(1110000)\rangle$ and the graph shown. No graph with explicit circulant symmetry exists.



$GF(4)$ representation of the stabilizer

Background: $GF(4)$ map for the stabilizer of an additive code:

$$U \equiv i^{m'} Z^{\mathbf{u}} X^{\mathbf{v}} \to (\mathbf{v}, \mathbf{u}) \to \mathbf{u} + \omega \mathbf{v},$$

where ω is the generator of $GF(4)$: $\overline{\omega} \equiv \omega^2 = \omega + 1$, $\overline{\omega}\omega = 1$.

Operators U_1 and U_2 commute iff

$$\mathbf{e}_1 * \mathbf{e}_2 \equiv \mathbf{e}_1 \cdot \overline{\mathbf{e}}_2 + \overline{\mathbf{e}}_1 \cdot \mathbf{e}_2 = \mathbf{v}_1 \cdot \mathbf{u}_2 + \mathbf{u}_1 \cdot \mathbf{v}_2.$$

Generator matrix for the additive $GF(4)$ code $\Leftrightarrow$ CWS code

$$G = P(\omega \mathbf{1} + R)$$

Parity check matrix for the binary code (P)

Graph adjacency matrix (R)

$GF(4)$ representation of the stabilizer

Background: $GF(4)$ map for the stabilizer of an additive code:

$$U \equiv i^{m'} Z^{\mathbf{u}} X^{\mathbf{v}} \rightarrow (\mathbf{v}, \mathbf{u}) \rightarrow \mathbf{u} + \omega \mathbf{v},$$

where ω is the generator of $GF(4)$: $\overline{\omega} \equiv \omega^2 = \omega + 1$, $\overline{\omega}\omega = 1$.

Operators U_1 and U_2 commute iff

$$\mathbf{e}_1 * \mathbf{e}_2 \equiv \mathbf{e}_1 \cdot \overline{\mathbf{e}}_2 + \overline{\mathbf{e}}_1 \cdot \mathbf{e}_2 = \mathbf{v}_1 \cdot \mathbf{u}_2 + \mathbf{u}_1 \cdot \mathbf{v}_2.$$

Generator matrix for the additive $GF(4)$ code $\Leftrightarrow$ CWS code

$$G = P(\omega \mathbf{1} + R)$$

Parity check matrix for the binary code → P

Graph adjacency matrix → R

G is automatically self-orthogonal as long as $R = R^{\mathrm{t}}$

$$G * \overline{G}^{\mathrm{t}} = P(\omega 1 + R) * (\overline{\omega} 1 + R) P^{\mathrm{t}} = 0$$

Gilbert-Varshamov bound for a given graph

Theorem: For a given graph $\mathcal{G}$ with the graph-state distance $d'(\mathcal{G})$, there is a binary code $\mathcal{C}$ such that the CWS code $\mathcal{Q} = (\mathcal{G}, \mathcal{C})$ is pure and satisfies the quantum Gilbert-Varshamov bound,

$$\sum_{s=1}^{d-1} 3^s \binom{n}{s} \leq 2^{n-k}, \text{ for } d \leq d'(\mathcal{G}).$$

Gilbert-Varshamov bound for a given graph

Theorem: For a given graph $\mathcal{G}$ with the graph-state distance $d'(\mathcal{G})$, there is a binary code $\mathcal{C}$ such that the CWS code $\mathcal{Q} = (\mathcal{G}, \mathcal{C})$ is pure and satisfies the quantum Gilbert-Varshamov bound,

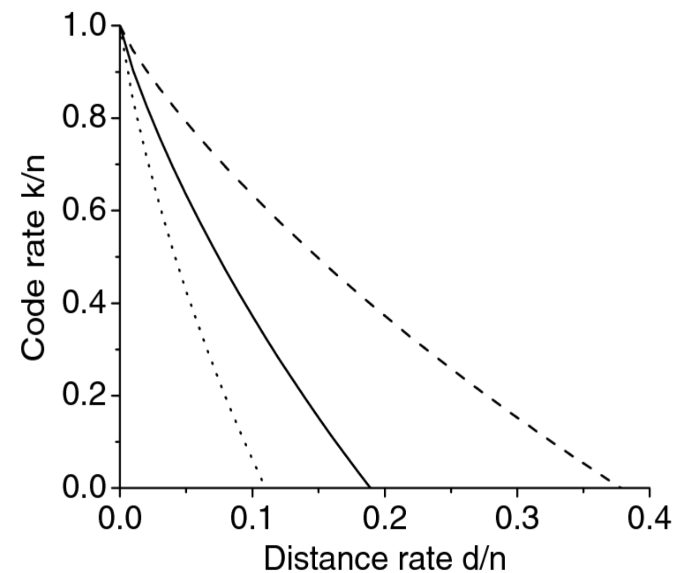
$$\sum_{s=1}^{d-1} 3^s \binom{n}{s} \leq 2^{n-k}, \text{ for } d \leq d'(\mathcal{G}).$$

- Once a suitable graph is chosen, one only has to find a binary code – much easier problem

When $n, k, d \to \infty$, relative distance $\delta = d/n$ and code rate $R = k/n$ satisfy

$$\delta \log_2 3 + H_2(\delta) \leq 1 - R,$$

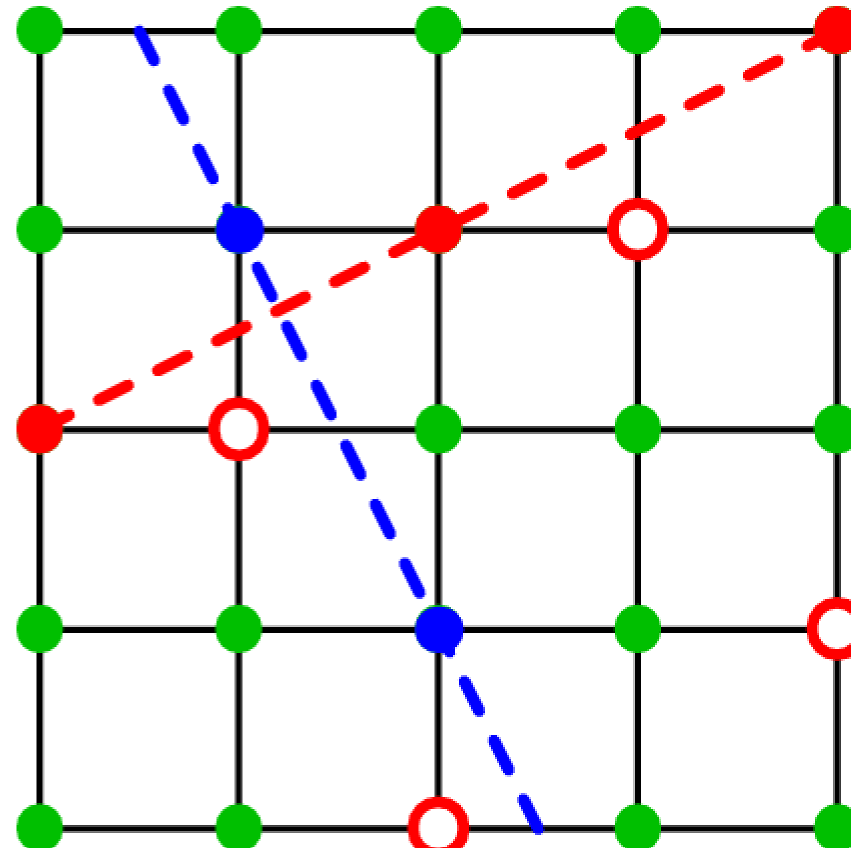
$$H_2(\delta) \equiv -\delta \log_2 \delta - (1-\delta) \log_2 (1-\delta)$$



Fixed distance codes

Gilbert-Varshamov bound for finite distance d implies the redundancy $n-k = d\log_2(3n/2d)$.

Example: Codes on finite square lattice have distance $d \leq 5$. With edges involved in the code, $d \leq 4$. Code $[[25,4,4]]$, member of the family $[[L_x L_y,(L_x-3)(L_y-3),4]]$. Redundancy $n-k = 3(L_x+L_y)-9 \propto \sqrt{n}$.

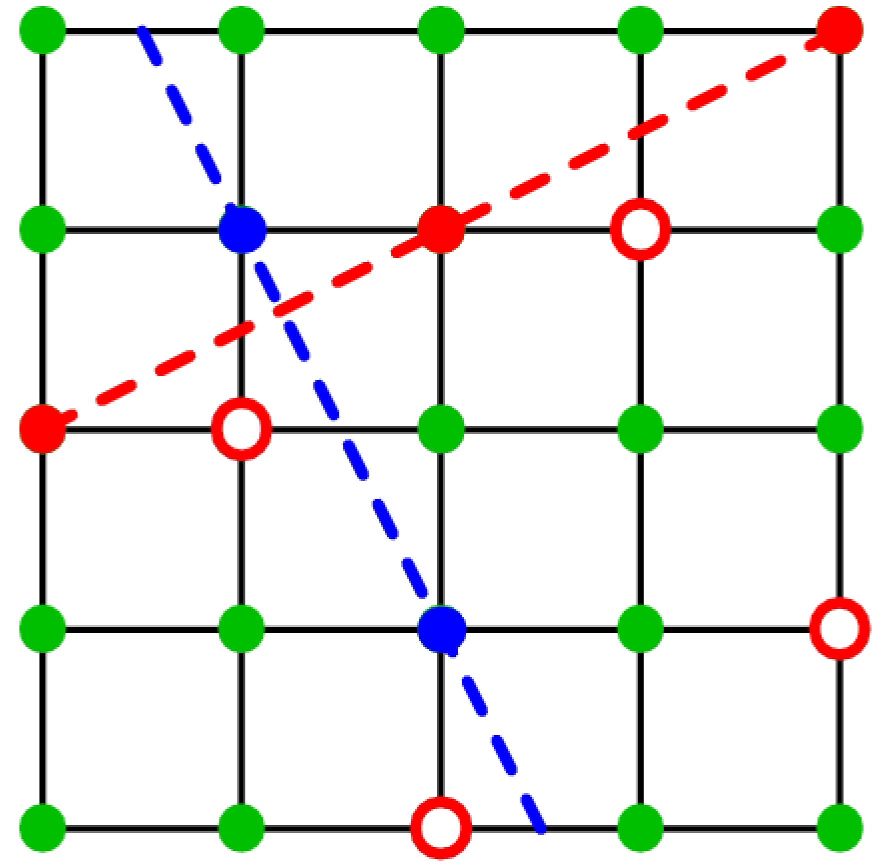


Codes found numerically: $\mathbf{[[25,10,5]]}$, $[[25,13,4]]$, $[[25,17,3]]$

Fixed distance codes

Gilbert-Varshamov bound for finite distance d implies the redundancy $n-k=d\log_2(3n/2d)$.

Example: Codes on finite square lattice have distance $d\leq 5$. With edges involved in the code, $d\leq 4$. Code $[[25,4,4]]$, member of the family $[[L_xL_y,(L_x-3)(L_y-3),4]]$. Redundancy $n-k=3(L_x+L_y)-9\propto\sqrt{n}$.



Codes found numerically: $[[\mathbf{25,10,5}]]$, $[[25,13,4]]$, $[[25,17,3]]$

Generalization: codes on a D-dimensional hypercubic lattice with $n=L^D$, $d=2D$, and redundancy $n-k\propto L^{D-1}$.

Cyclic CWS & related codes

Cyclic code: $(ZYYZI) \in \mathscr{S} \rightarrow (IZYYZ) \in \mathscr{S}$.

Circulant matrix $G = \begin{pmatrix} 1 & \overline{\omega} & \overline{\omega} & 1 & \cdot \\ \cdot & 1 & \overline{\omega} & \overline{\omega} & 1 \\ 1 & \cdot & 1 & \overline{\omega} & \overline{\omega} \\ \overline{\omega} & 1 & \cdot & 1 & \overline{\omega} \\ \overline{\omega} & \overline{\omega} & 1 & \cdot & 1 \end{pmatrix}$

Map: circulant matrix $\rightarrow$ polynomial $g(x) = 1 + \bar{\omega}x + \bar{\omega}x^2 + x^3$

Shift: $g(x) \rightarrow xg(x) \mod (x^n - 1)$

Cyclic CWS & related codes

Cyclic code: $(ZYYZI) \in \mathscr{S} \rightarrow (IZYYZ) \in \mathscr{S}$.

Circulant matrix $G = \begin{pmatrix} 1 & \overline{\omega} & \overline{\omega} & 1 & \cdot \\ \cdot & 1 & \overline{\omega} & \overline{\omega} & 1 \\ 1 & \cdot & 1 & \overline{\omega} & \overline{\omega} \\ \overline{\omega} & 1 & \cdot & 1 & \overline{\omega} \\ \overline{\omega} & \overline{\omega} & 1 & \cdot & 1 \end{pmatrix}$

Map: circulant matrix $\rightarrow$ polynomial $g(x) = 1 + \bar{\omega}x + \bar{\omega}x^2 + x^3$

Shift: $g(x) \rightarrow xg(x) \mod (x^n - 1)$

Additive CWS code: $G = P(\omega\mathbf{1} + R)$, $R^{\mathrm{t}} = R$.

CWS cyclic code: $g(x) = p(x)(\omega + r(x))$,
where $r(x)$ is symmetric, $r(x^{n-1}) = r(x) \mod (x^n - 1)$, and
$p(x)$ is a factor of $x^n - 1$, $p(x)q(x) = x^n - 1$.

Example: $[[5, 1, 3]]$ code $p(x) = 1 + x$, $r(x) = x + x^4$.

Cyclic CWS & related codes

Cyclic code: $(ZYYZI) \in \mathscr{S} \to (IZYYZ) \in \mathscr{S}$.

Circulant matrix $G = \begin{pmatrix} 1 & \overline{\omega} & \overline{\omega} & 1 & \cdot \\ \cdot & 1 & \overline{\omega} & \overline{\omega} & 1 \\ 1 & \cdot & 1 & \overline{\omega} & \overline{\omega} \\ \overline{\omega} & 1 & \cdot & 1 & \overline{\omega} \\ \overline{\omega} & \overline{\omega} & 1 & \cdot & 1 \end{pmatrix}$

Map: circulant matrix $\to$ polynomial $g(x) = 1 + \bar{\omega}x + \bar{\omega}x^2 + x^3$

Shift: $g(x) \to xg(x) \mod (x^n - 1)$

Additive CWS code: $G = P(\omega\mathbf{1} + R)$, $R^{\mathrm{t}} = R$.

CWS cyclic code: $g(x) = p(x)(\omega + r(x))$,
where $r(x)$ is symmetric, $r(x^{n-1}) = r(x) \mod (x^n - 1)$, and
$p(x)$ is a factor of $x^n - 1$, $p(x)q(x) = x^n - 1$.

Example: $[[5, 1, 3]]$ code $p(x) = 1 + x$, $r(x) = x + x^4$.

General one-generator cyclic codes
$p(x)p(x^{n-1})r(x^{n-1}) = p(x)p(x^{n-1})r(x) \mod x^n - 1.$

Lower GV bound for cyclic quantum codes

Consider a binary cyclic code $\mathcal{C}[n,k,d_{\mathcal{C}}]$ with the generator polynomial $q(x)$ which is irreducible. Then there exists a quantum cyclic code $\mathcal{Q}[n,k,d]$, with $d=\min(d_{\mathcal{C}},d')$, where $d'=d_{\mathrm{GV}}(n,k)$ is (a somewhat improved) Gilbert-Varshamov bound if $q(x)$ is non-palindromic,

$$d_{\mathrm{GV}}(n,k)\equiv \max d:\sum_{s=1}^{d-1}(3^s-3)\frac{\gcd(s,n)}{n}\binom{n}{s}\le 2^{n-k}-2,$$

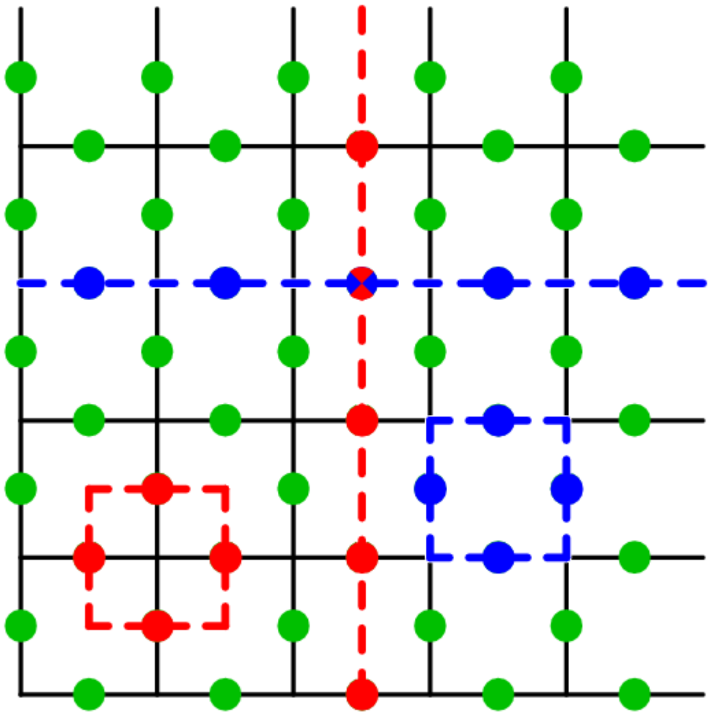
while for a palindromic $q(x)$, $x^{\deg q(x)}q(1/x)=q(x)$,

$$d'\approx d_{\mathrm{GV}}(n/2,k/2)\ge \frac{1}{2}d_{\mathrm{GV}}(n,k).$$

Example: existence proofs

Standard Gilbert-Varshamov bound for a finite number of encoded qubits k implies a finite relative distance $d/n \geq 0.189, \quad n \to \infty$

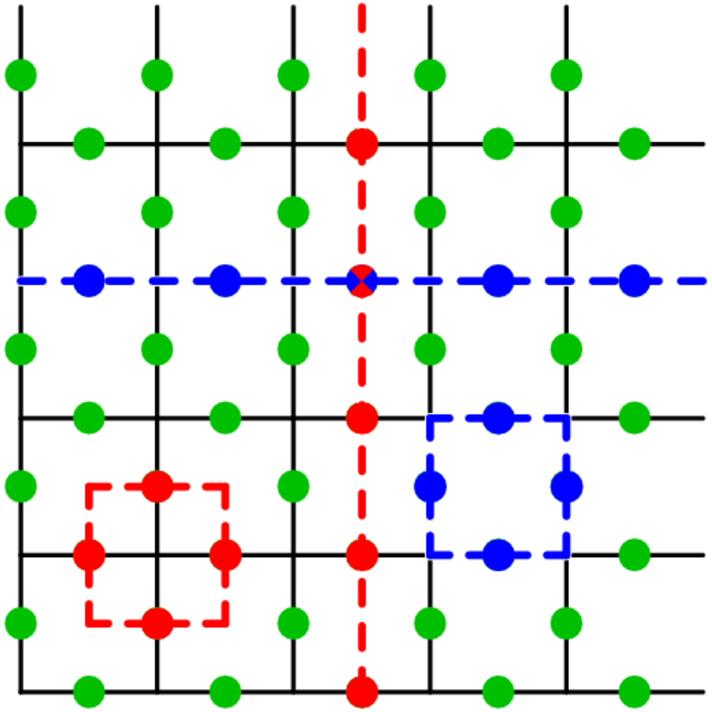
Toric codes: $[[n = 2L^2, k = 2, d = L]]$: $d/n \propto 1/\sqrt{n}$
$[[18, 2, 3]]$, $[[50, 2, 5]]$, $[[98, 2, 7]]$, ...



Example: existence proofs

Standard Gilbert-Varshamov bound for a finite number of encoded qubits k implies a finite relative distance $d/n \geq 0.189, \quad n \to \infty$

Toric codes: $[[n = 2L^2, k = 2, d = L]]$: $d/n \propto 1/\sqrt{n}$
$[[18, 2, 3]]$, $[[50, 2, 5]]$, $[[98, 2, 7]]$, $\ldots$

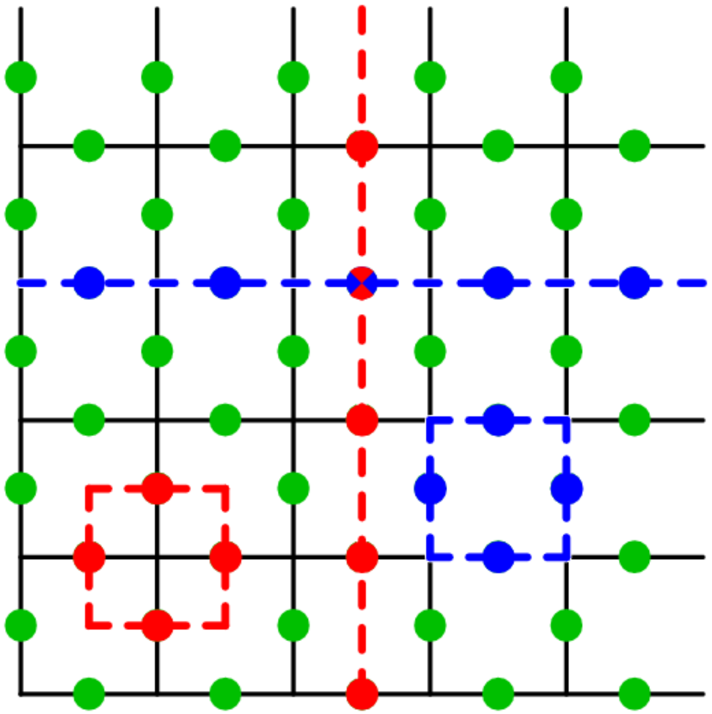


For $n \lesssim 50$, most "good" quantum cyclic codes have $dk = n$, including many codes with small-weight stabilizer generators. Obtained from k replicas of the classical repetition codes $[kd, k, d]$.

Example: existence proofs

Standard Gilbert-Varshamov bound for a finite number of encoded qubits k implies a finite relative distance $d/n \geq 0.189, \quad n \to \infty$

Toric codes: $[[n = 2L^2, k = 2, d = L]]$: $d/n \propto 1/\sqrt{n}$
$[[18, 2, 3]]$, $[[50, 2, 5]]$, $[[98, 2, 7]]$, $\ldots$

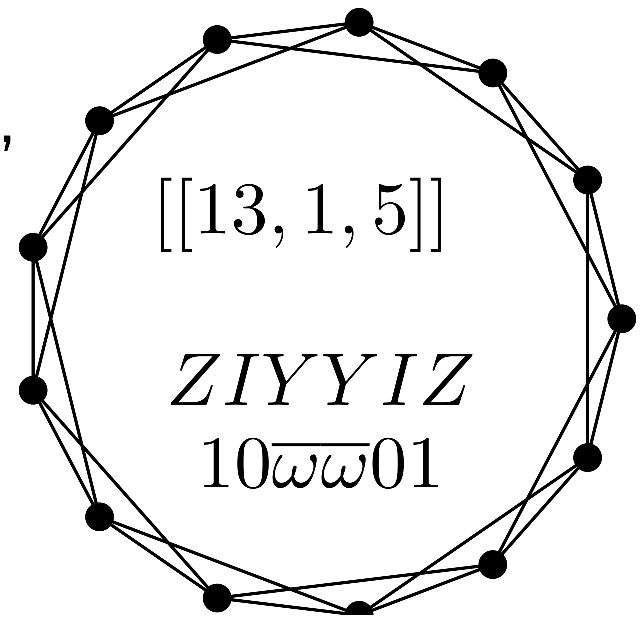


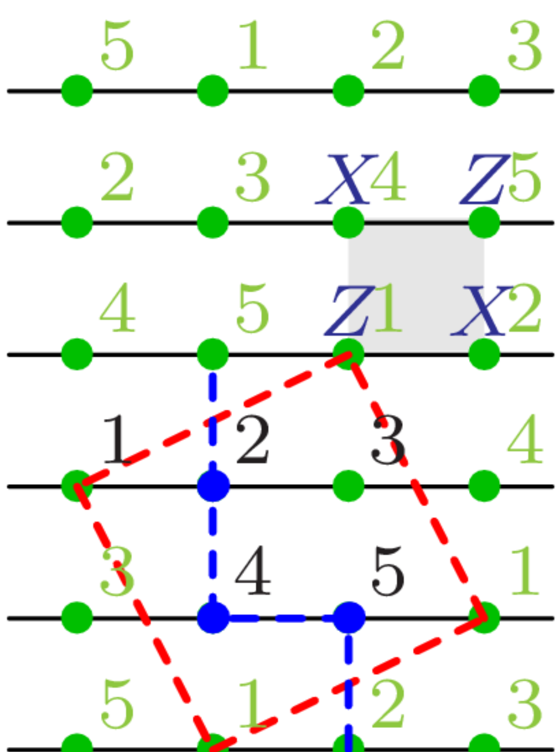
For $n \lesssim 50$, most "good" quantum cyclic codes have $dk = n$, including many codes with small-weight stabilizer generators. Obtained from k replicas of the classical repetition codes $[kd, k, d]$.

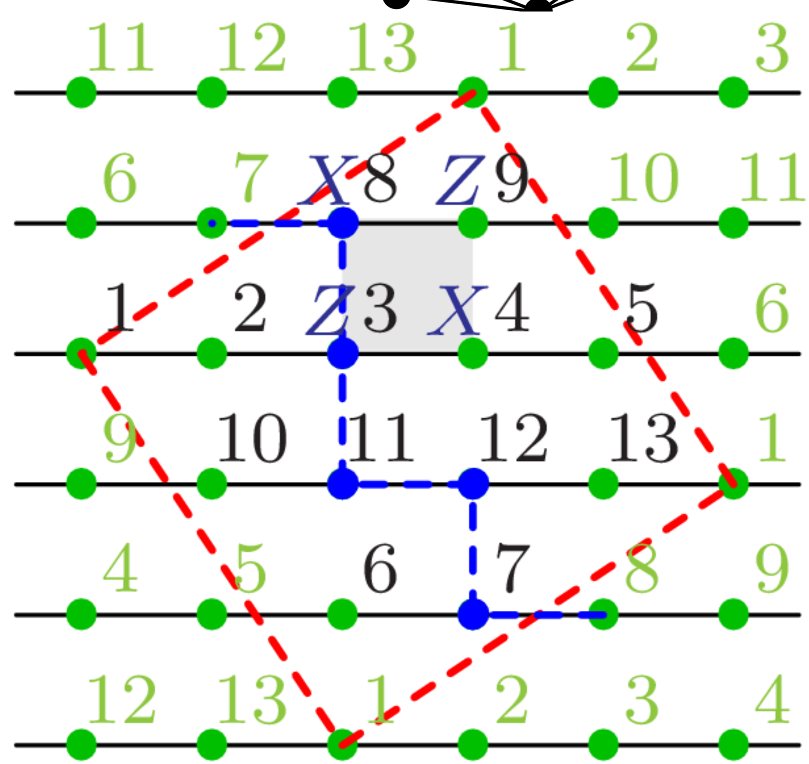
Codes corresponding to binary BCH codes:
$[[23, 12, 4]]$, $[[47, 24, d \geq 6]]$, $[[71, 36, d \geq 7]]$,
$[[95, 59, 5]]$, $[[115, 71, 5]]$, $[[143, 83, 11]]$, $\ldots$

Example: cyclic toric-like codes

Take $p(x) = 1 + x$ and
$n = t^2 + (t+1)^2 = t + 2 + (t+1)(2t-1)$,
$t = 1, 2, \ldots$ ($n = 5, 13, 25, 41, \ldots$) $\Rightarrow$ two code families $[[n, 1, d]]$ with $d = 2t + 1$:
$ZYIYZ$, $ZYIIIYZ$, $ZYIIIIIYZ$, $\ldots$
$ZYYZ$, $ZIYYIZ$, $ZIIYYIIZ$, $\ldots$
Largest distance codes with weight-4 generators.







Conclusions

- Non-additive CWS codes are difficult to correct.
- Find additive CWS codes via divide and conquer approach: $\mathcal{G} \to \mathcal{Q} = (\mathcal{G}, \mathcal{C})$.
  - Lower compexity compared to full search; Ok codes.
  - Use regular lattices to build finite-distance codes.
- Cyclic CWS codes $\subset$ One-generator cyclic codes.
  - Large class of easy-to construct quantum codes
  - Include codes with small-weight stabilizer
  - Rotated surface codes & friends – see Poster.
  - $[[5, 1, 3]]$ code gets a torus.