Topics

- Spatially-Coupled Chaos System
- Spatially-Coupled SUDOKU
- Quantum Codes
- Duality

Acknowledgement

First two topics are motivated by the talk of T. Tanaka.

“Mathematics of \((X)^n\),” Workshop on Spatially Coupled Codes and Related Topics, Tokyo Tech, Feb. 2011.

- We have investigated interesting properties of many large systems so far. \(X = x^n\) e.g., LDPC codes, \(k\)-SAT, spin glass.
- Substitute anything to \(X\). Do coupled systems \((X)^L\) behave differently from \(X\)?
Chaos System

Logistic Map [R. May]

$x_t$ is the population of insects of the $t$-th generation.

$\alpha$ is a constant in $[0, 4]$.

$$x_{t+1} = \alpha x_t (1 - x_t)$$

- Behavior depends highly on $\alpha$.
- For $\alpha < \alpha^* \approx 3.5699456$ $x_t$ takes periodic values.
- For $\alpha > \alpha^* \approx 3.5699456$ $x_t$ takes un-periodic values.
Spatially-Coupled Chaos System

Coupled Logistic Maps

\[ x_{t+1, i} = \begin{cases} \alpha \left( \frac{1}{2w+1} \sum_{j=-w}^{w} x_{t, i+j} \right) \left( 1 - \frac{1}{2w+1} \sum_{j=-w}^{w} x_{t, i+j} \right) & i \in [0, L - 1] \\ 0 & i \notin [0, L - 1] \end{cases} \]

Coupled Logistic Maps (L=9, 2w+1=3)

Open Problems

- The point \( \alpha^* \) is changed?
- Applications?
SUDOKU

- Constraint-satisfaction problem like K-SAT problem.
- Each column, each row, and each of the nine 3 sub-grids contains 1, ..., 9.
- Helps many people in flight.
- Iterative decoding is possible.
- The factor graph of SUDOKU is not sparse.
- The possible number of SUDOKU grid is about $6.671 \times 10^{21}$. 

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>3</td>
<td>1</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>2</td>
<td>9</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>9</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>3</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
</tr>
</tbody>
</table>
Generalized SUDOKU

<table>
<thead>
<tr>
<th>L</th>
<th>U</th>
<th>K</th>
<th>G</th>
<th>C</th>
<th>Q</th>
<th>I</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q</td>
<td>H</td>
<td>R</td>
<td>K</td>
<td>V</td>
<td>AM</td>
<td>T</td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>A</td>
<td>B</td>
<td>H</td>
<td>C</td>
<td>X</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>U</td>
<td>V</td>
<td>X</td>
<td>W</td>
<td>D</td>
<td>J</td>
<td>E</td>
<td>I</td>
</tr>
<tr>
<td>K</td>
<td>G</td>
<td>X</td>
<td>F</td>
<td>B</td>
<td>W</td>
<td>Q</td>
<td>D</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q</th>
<th>I</th>
<th>U</th>
<th>O</th>
<th>S</th>
<th>R</th>
<th>P</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td>D</td>
<td>V</td>
<td>K</td>
<td>J</td>
<td>P</td>
<td>Q</td>
<td>L</td>
</tr>
<tr>
<td>F</td>
<td>C</td>
<td>R</td>
<td>A</td>
<td>N</td>
<td>U</td>
<td>G</td>
<td>I</td>
</tr>
<tr>
<td>I</td>
<td>Q</td>
<td>H</td>
<td>O</td>
<td>Y</td>
<td>L</td>
<td>D</td>
<td>B</td>
</tr>
<tr>
<td>M</td>
<td>G</td>
<td>W</td>
<td>C</td>
<td>T</td>
<td>J</td>
<td>R</td>
<td>D</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>M R</th>
<th>E</th>
<th>B</th>
<th>D</th>
<th>C</th>
<th>H</th>
<th>A</th>
<th>G</th>
<th>W</th>
</tr>
</thead>
<tbody>
<tr>
<td>P W</td>
<td>G</td>
<td>A</td>
<td>Y</td>
<td>E</td>
<td>X</td>
<td>N</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K Y</td>
<td>L</td>
<td>W</td>
<td>U</td>
<td>T</td>
<td>N</td>
<td>D</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H L</td>
<td>T</td>
<td>S</td>
<td>W</td>
<td>V</td>
<td>K</td>
<td>X</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>N B</td>
<td>H</td>
<td>S</td>
<td>Y</td>
<td>F</td>
<td>P</td>
<td>C</td>
<td>E</td>
<td></td>
</tr>
<tr>
<td>L Q</td>
<td>E</td>
<td>U</td>
<td>R</td>
<td>F</td>
<td>B</td>
<td>I</td>
<td>X</td>
<td>D</td>
</tr>
<tr>
<td>B A</td>
<td>C</td>
<td>Y</td>
<td>S</td>
<td>U</td>
<td>V</td>
<td>P</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>T X</td>
<td>P</td>
<td>J</td>
<td>Q</td>
<td>A</td>
<td>W</td>
<td>E</td>
<td>R</td>
<td>Y</td>
</tr>
<tr>
<td>H N</td>
<td>Y</td>
<td>Q</td>
<td>X</td>
<td>I</td>
<td>S</td>
<td>E</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>K Y</td>
<td>F</td>
<td>T</td>
<td>A</td>
<td>G</td>
<td>P</td>
<td>N</td>
<td>J</td>
<td>O</td>
</tr>
<tr>
<td>V W</td>
<td>U</td>
<td>P</td>
<td>H</td>
<td>R</td>
<td>G</td>
<td>X</td>
<td>N</td>
<td>M</td>
</tr>
<tr>
<td>G O</td>
<td>T</td>
<td>F</td>
<td>X</td>
<td>B</td>
<td>N</td>
<td>M</td>
<td>K</td>
<td>C</td>
</tr>
<tr>
<td>C U</td>
<td>J</td>
<td>G</td>
<td>Y</td>
<td>N</td>
<td>O</td>
<td>S</td>
<td>I</td>
<td>V</td>
</tr>
<tr>
<td>I R</td>
<td>E</td>
<td>W</td>
<td>S</td>
<td>O</td>
<td>J</td>
<td>A</td>
<td>K</td>
<td></td>
</tr>
<tr>
<td>P T</td>
<td>C</td>
<td>X</td>
<td>M</td>
<td>D</td>
<td>Q</td>
<td>Y</td>
<td>U</td>
<td>L</td>
</tr>
</tbody>
</table>

- \((n^2) \times (n^2)\) generalization.
- The possible numbers of generalized SUDOKU grid is open.
- Asymptotic behaviour \(n \rightarrow \infty\) of possible number is known in part.
- Iterative decoding is still possible.

25 × 25 SUDOKU
Locally a coupled SUDOKU is equivalent with an uncoupled SUDOKU.

Constraints at boundaries are weaker and help iterative decoding.

Open Problems

- Coupling helps the iterative decoder?
- Coupling helps in counting the possible SUDOKU numbers?
CSS(Calberbank, Shor, Steane) Codes

CSS codes are a class of quantum codes. A CSS code is a quantum codes which is constructed from a classical binary codes pair \((C, D)\).

Underlying two classical codes are required to satisfy

- \(C^\perp \subset D\) and \(D^\perp \subset C\)
- In other words, \(H_C H_D^T = 0\)

On top of that, in this research, we request the followings.

- \(H_C\) are \(H_D\) sparse.
- \(C\) and \(D\) are efficiently decodable by sum-product algorithms.
Quasi-Cyclic LDPC Codes

A \((J, L, P)\) quasi-cyclic LDPC code \(C\) is defined by binary a parity-check matrix \(H_C\) as follows

\[
H_C = \begin{bmatrix}
I(c_{0,0}) & I(c_{0,1}) & \cdots & I(c_{0,L-1}) \\
I(c_{1,0}) & I(c_{1,1}) & \cdots & I(c_{1,L-1}) \\
\vdots & \vdots & \ddots & \vdots \\
I(c_{J-1,0}) & I(c_{J-1,1}) & \cdots & I(c_{J-1,L-1})
\end{bmatrix}
\]

\(H_C\) is a binary matrix which consists of \(J \times L\) sub-matrices of size \(P \times P\).

where

\[
I(1) = \begin{bmatrix}
1 \\
& 1 \\
& & \ddots \\
& & & 1
\end{bmatrix} \in \{0, 1\}^{P \times P}
\]

\(I(c)\) is a cyclically-shifted identity matrix by \(c\).

\(I(c) := I(1)^c, c \in [0, P]\)
Input: \((J, L, P)\)  
Output: \((J, L, P)\) QC-LDPC CSS code \((C, D)\)

**STEP 1:** Pick two integers \(\sigma, \tau_1, \tau_2 \in \mathbb{Z}_P^*\) such that

\[
\begin{align*}
L/2 &= \text{ord}(\sigma), \\
1 &\leq J \leq \text{ord}(\sigma), \\
\text{ord}(\sigma) &\neq \#\mathbb{Z}_P^*, \\
1 - \sigma^j &\in \mathbb{Z}_P^* \text{ for all } 1 \leq j < \text{ord}(\sigma), \\
\tau_2 &\neq \tau_1, \tau_1 \sigma, \tau_1 \sigma^2, \ldots, \tau_1 \sigma^{\text{ord}(\sigma)-1},
\end{align*}
\]

where \(\mathbb{Z}_P^* := \{z \in \mathbb{Z}_P \mid \exists a \in \mathbb{Z}_P, za = 1\}\),  
\(\text{ord}(\sigma) := \min\{m > 0 \mid \sigma^m = 1\}\).

**STEP 2:** Construct \(H_C\)

\[
H_C = (l(c_{j, \ell}))_{0 \leq j < J, 0 \leq \ell < L},
\]

\[
c_{j, \ell} := \begin{cases} 
\sigma^{-j+\ell} & 0 \leq \ell < L/2 \\
\tau \sigma^{-j+\ell} & L/2 \leq \ell < L,
\end{cases}
\]

**STEP 3:** Construct \(H_D\)

\[
H_D = (l(d_{j, \ell}))_{0 \leq j < J, 0 \leq \ell < L},
\]

\[
d_{j, \ell} := \begin{cases} 
-\tau \sigma^{j-\ell} & 0 \leq \ell < L/2 \\
-\sigma^{j-\ell} & L/2 \leq \ell < L,
\end{cases}
\]
Coupled Quantum Codes

\[
H_C = \begin{bmatrix}
16 & 18 & 28 & 4 & 20 & 7 \\
28 & 16 & 18 & 7 & 4 & 20 \\
18 & 28 & 16 & 20 & 7 & 4 \\
9 & 14 & 8 & 29 & 21 & 12 \\
6 & 30 & 26 & 1 & 5 & 25 \\
30 & 26 & 6 & 5 & 25 & 1 \\
15 & 13 & 3 & 15 & 13 & 11 \\
27 & 11 & 14 & 17 & 23 & 22 \\
24 & 11 & 7 & 6 & 30 & 26 \\
4 & 20 & 7 & 30 & 26 & 6 \\
2 & 10 & 19 & 17 & 23 & 19 \\
2 & 10 & 19 & 17 & 23 & 19 \\
6 & 30 & 26 & 4 & 20 & 7 \\
23 & 22 & 17 & 10 & 19 & 2 \\
26 & 6 & 30 & 7 & 4 & 20 \\
30 & 26 & 6 & 20 & 7 & 4
\end{bmatrix}
\]

\[
H_D = \begin{bmatrix}
\end{bmatrix}
\]

Designed so that
- Couple Hagiwara-Imai codes.
- \(H_C H_D^T = 0\)
- \(H_C\) and \(H_D\) have no cycles of length 4.

Enjoys at the same time
- deep error-floors with large row-weight.
- good water-fall with large row-weight.

Open Problem
- Coupled quantum codes still leave a gap to the theoretical limit.
- Need more randomness?
Duality

Definition of Dual Code

\[
C^\perp = \{ x \in \mathbb{F}_2^n | \langle x, c \rangle = 0 \ \forall c \in C \}, \text{ where } \langle x, c \rangle = \sum_{i=1}^{n} x_i c_i
\]

- Duality is mathematically interesting.
- Duality is important for quantum codes.

Open Problem

Efficiently-decodable capacity-achieving \( C \) and \( C^\perp \) exist? Self-dual?

Known facts

- If \( C \) achieves the capacity under MAP decoding, then \( C^\perp \) also achieves the capacity under MAP decoding.
- The dual code of a polar code does not achieve the capacity under successive cancellation decoding. (Thanks to R. Mori)
MacKay-Neal codes

\( H_1 \): a \((d_v, d_c)\)-regular \( N \times \frac{d_c}{d_v} N \) random sparse matrix.

\( H_2 \): a \((d_g, d_g)\)-regular \( N \times N \) random sparse matrix.

A \((d_v, d_c, d_g)\)-MN code is defined by a generator matrix

\[
G_{MN} = H_1^T \left( H_2^{-1} \right)^T \in \{0, 1\} \frac{d_c}{d_v} N \times N.
\]

Hsu-Anastasopoulos codes

\( H_3^T \): a \((d'_v, d'_c)\)-regular \( \frac{d'_c}{d'_v} N \times N \) random sparse matrix

\( H_4^T \): a \((d_g, d_g)\)-regular \( N \times N \) random sparse matrix

A \((d'_v, d'_c, d_g)\)-HA code is defined by a parity-check matrix

\[
H_{HA} = H_3^T \left( H_4^T \right)^{-1} \in \{0, 1\} \frac{d'_c}{d'_v} N \times N.
\]

If we set \( d_v = d'_c, d_c = d'_v, H_1 = H_3 \) and \( H_2 = H_4 \), it holds \( G_{MN} = H_{HA} \).

It follows the \((d'_v, d'_c, d_g)\)-HA code is dual code of the \((d_v, d_c, d_g)\)-MN code.