Graph states and unitary transforms

Constanza Riera Burger

University of Bergen

Madrid, Thursday 20th 2007

Outline

Motivation

- Graph states $\rightarrow$ measurement-based quantum computing
- Unitary transforms: act in quantum states and may change entanglement
- Some unitary transforms generate the significant part of the Local Clifford Group: set $\{I, H, N\}^n$
- Graph states: representable by a graph, a quadratic boolean function, a matrix...
- We represent the orbit of graph states w.r.t. $\{I, H, N\}^n$ as graph transforms $\rightarrow$ faster computation

Quantum states and unitary matrices

- Quantum state in n qubits $=$ vector in the Hilbert space $\mathbb{C}^{2^n}$
- Unitary transform $=$ complex unitary matrix $2^n \times 2^n$

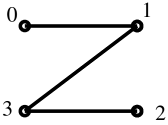
Boolean functions, graphs and matrices

Different interpretations of a quadratic Boolean function:

- ANF: $p(\mathbf{x}) = \sum_{0 \le i < j \le n-1} a_{ij} x_i x_j$
- Graph: Define G as:
  - Vertices: $\{0, \cdots, n-1\}$
  - Edges: There is an edge between i and j iff $a_{ij} = 1$
- Graph state: take $x_0, \ldots, x_{n-1}$ as n qu-bits: $\frac{1}{2^n}(-1)^p$ is a quantum state

Example

ANF: $p(\mathbf{x}) = x_0x_1 + x_1x_3 + x_2x_3$
Graph G:



Example(cont.)

$$\text{Graph state: } |\varphi\rangle = \frac{1}{4}\begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \\ 1 \\ -1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ -1 \\ -1 \\ 1 \\ -1 \\ -1 \end{pmatrix} \in \mathbb{C}^{2^4}$$

Spectrum of a boolean function

- I is the 2×2 identity matrix
- $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ the *Walsh-Hadamard kernel*
- $N = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$ the *Negahadamard kernel*
- Let $U \in \{I, H, N\}$. Then,

$$U_j = I \otimes \cdots \otimes I \otimes U \otimes I \otimes \cdots \otimes I \quad ,$$

where the U occurs in position j in the tensor product.

Spectrum of a function

- $\{I, H, N\}^n$ is the set of U:

$$U = \prod_{j \in \mathbf{R_I}} I_j \prod_{j \in \mathbf{R_H}} H_j \prod_{j \in \mathbf{R_N}} N_j$$

where the sets $\mathbf{R_I}, \mathbf{R_H}$ and $\mathbf{R_N}$ partition the set of vertices $\{0, \ldots, n-1\}$

Spectrum of a function

- The spectrum of $p(\mathbf{x})$ w.r.t. the transform U is the vector $P_U = (P_{U,\mathbf{k}}) \in \mathbb{C}^{2^n}$, where

$$P_U = U(-1)^{p(\mathbf{x})} = \left(\prod_{j \in \mathbf{R_I}} I_j \prod_{j \in \mathbf{R_H}} H_j \prod_{j \in \mathbf{R_N}} N_j \right) (-1)^{p(\mathbf{x})}$$

- $p(\mathbf{x})$ has a flat spectrum w.r.t. U if $|P_{U,\mathbf{k}}| = 1 \ \forall \ \mathbf{k}$
- WHT: $U = \bigotimes_{i=0}^{n-1} H \Rightarrow P_{U,\mathbf{k}} = \frac{1}{2^{n/2}} \sum_{\mathbf{x} \in GF(2)^n} (-1)^{p(\mathbf{x}) + \mathbf{k} \cdot \mathbf{x}}$

  Flat spectrum w.r.t. $\bigotimes_{i=0}^{n-1} H$ iff Bent

Example

$p(x) = x_0 x_1$. Then, if $U = H \otimes H$,

$$P_U = U(-1)^{p(x)} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix}$$

$|P_{U,\mathbf{k}}| = 1 \ \forall \ \mathbf{k} \Rightarrow p(x)$ has a flat spectrum w.r.t. $H \otimes H \Rightarrow$ Bent

Two-graphs state

- APF: $|\psi\rangle = cm(\mathbf{x})(-1)^{p(\mathbf{x})}$, with $c \in \mathbb{C}$, and $m, p : \mathbb{Z}_2^n \to \mathbb{Z}_2$ Boolean functions, m product of affine boolean functions
- magnitude: m
- phase: p

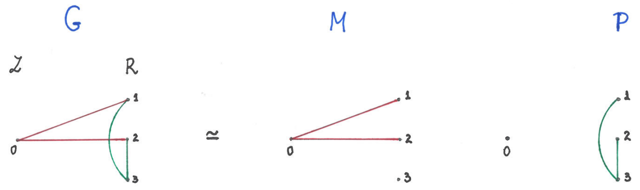
Two-graphs state

If we have $s = cm(-1)^p$ then:

$$\left.\begin{array}{l} m \leftrightarrow M \text{ graph} \\ p \leftrightarrow P \text{ graph} \end{array}\right\} \Leftrightarrow \left\{\begin{array}{l} (G, \mathcal{R}) \text{ where} \\ P = G_{\mathcal{R}}, M = G - P \end{array}\right.$$

Example

$$p(x) = x_1x_3 + x_2x_3,\ m = x_0 + x_1 + x_2 + 1,\ s = m(-1)^p$$

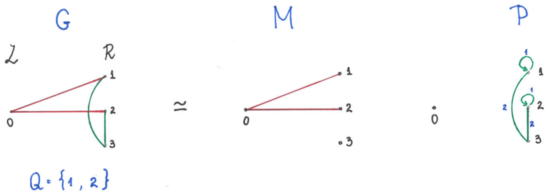


Example(cont.)

$$\text{Two-Graph state: } |\varphi\rangle = \frac{1}{4}\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ -1 \\ 1 \\ -1 \\ 0 \\ 1 \end{pmatrix} \in \mathbb{C}^{2^4}$$

Generalised Two-Graph State

- Two-graph state is not enough: the action of N can create some $\mathbb{Z}_4$ linear terms in the spectrum.
- Two-graph state: $(G, \mathcal{R}, \mathcal{Q})$, where $\mathcal{Q}$ represents the $\mathbb{Z}_4$ linear terms.
- Example: $p(x) = 2x_1x_3 + 2x_2x_3 + x_1 + x_2$, $m = x_0 + x_1 + x_2 + 1$, $s = mi^p$



Example(cont.)

Genaralised Two-Graph state: $|\varphi\rangle = \frac{1}{4}\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ i \\ -i \\ i \\ -i \\ 0 \\ 1 \end{pmatrix} \in \mathbb{C}^{2^4}$

Edge Local Complementation$^\odot$ (ELC$^\odot$)

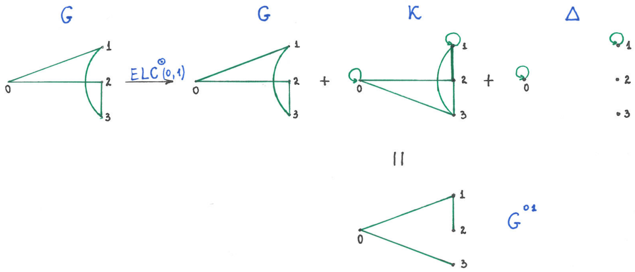
Definition

Let G be a graph with possible loops, containing an edge vw, $v \neq w$. Then G^{vw} is the graph resulting from the action of edge local complementation$^\odot$ *(ELC$^\odot$) on edge vw of G, where*

$$G^{vw} = G + K_{\mathcal{B}_v,\mathcal{B}_w} + \Delta_{\{v,w\}} + \Gamma_{G_{vv}} \Delta_{\mathcal{B}_w^G} + \Gamma_{G_{ww}} \Delta_{\mathcal{B}_v^G} \ .$$

Example

- Example:



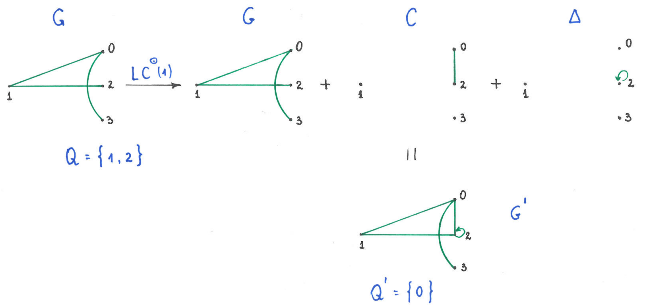
Local Complementation$^{\odot}$ (LC$^{\odot}$)

Definition

Let $(G, \mathcal{Q})$ be a graph-set pair with G an n-vertex graph with possible loops and $\mathcal{Q} \subset \{0, 1, \ldots, n-1\}$. Then $(G, \mathcal{Q})^v = (G^v, \mathcal{Q}^v)$ is the graph-set pair resulting from the action of local complementation$^{\odot}$ *(LC$^{\odot}$) on vertex v of $(G, \mathcal{Q})$, where*

$$G^v = G + C_{\mathcal{N}_v^G} + \Gamma_{G_{vv}} \Delta_{\mathcal{N}_v^G} + \Delta_{\mathcal{Q} \cap \mathcal{N}_v^G},$$
$$\mathcal{Q}^v = \mathcal{Q} \ominus \mathcal{B}_v^G.$$

Example



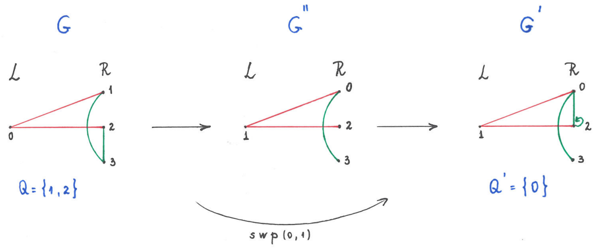
Action of '$swp(v, w)'$ on a generalised two-graph state

- swp (v, w) interchanges the roles of v and w: takes $\mathcal{R}$ to $\mathcal{R}' = \mathcal{R} \cup \{v\} \setminus \{w\}$
- the state does not change but m and p do change, as does the graphical representation

Lemma

$$\begin{cases} \mathcal{R}' = \mathcal{R} \cup \{v\} \setminus \{w\}, \\ G'' = G^{vw}, \\ \textit{if } \mathcal{Q}_w = 1 \\ \qquad (G, \mathcal{Q})' = (G'', \mathcal{Q})^w \\ \textit{else} \\ \qquad (G, \mathcal{Q})' = (G'', \mathcal{Q}) \end{cases}$$

Example



Action of H on a generalised two-graph state

Theorem

$$\begin{cases} \mathcal{R}' = \mathcal{R} \cup \{v\}, \\ (G, \mathcal{Q})' = (G, \mathcal{Q}), \end{cases} \qquad \text{if } v \in \mathcal{L},$$

$$\begin{cases} \text{if } \mathcal{Q}_v = 0 \\ \qquad \mathcal{R}' = \mathcal{R} \setminus \{v\}, \\ \qquad (G, \mathcal{Q})' = (G, \mathcal{Q}), \\ \text{if } \mathcal{Q}_v = 1 \\ \qquad \mathcal{R}' = \mathcal{R}, \\ \qquad (G'', \mathcal{Q}'') = (G, \mathcal{Q})^v \\ \qquad G' = G'' + \Delta_{\mathcal{B}_v^G} \\ \qquad \mathcal{Q}' = \mathcal{Q}'' \cup \{v\} \end{cases}, \qquad \text{if } \mathcal{B}_v^G \subset \mathcal{R}$$

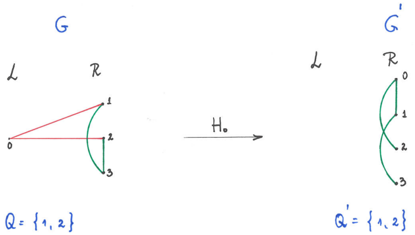
Action of H on a generalised two-graph state (cont.)

Theorem (cont.)

$$\begin{cases} \text{for } w \in \mathcal{N}_v^M, & \\ \quad (G', \mathcal{R}'', \mathcal{Q}') = swp(G, \mathcal{R}, \mathcal{Q}, w, v), & \text{if } v \in \mathcal{R}, \mathcal{B}_v^G \not\subset \mathcal{R} \\ \quad \mathcal{R}' = \mathcal{R}'' \cup \{v\}. & \end{cases}$$

Example

$$\begin{cases} \mathcal{R}' = \mathcal{R} \cup \{v\} \\ (G, \mathcal{Q})' = (G, \mathcal{Q}) \end{cases}$$



Action of N on a generalised two-graph state

Theorem

$$\begin{cases} \mathcal{R}' = \mathcal{R} \cup \{v\}, \\ (G', \mathcal{Q}'') = (G, \mathcal{Q})^v, \\ \mathcal{Q}' = \mathcal{Q}'' \setminus \{v\}, \end{cases} \qquad \text{if } v \in \mathcal{L},$$

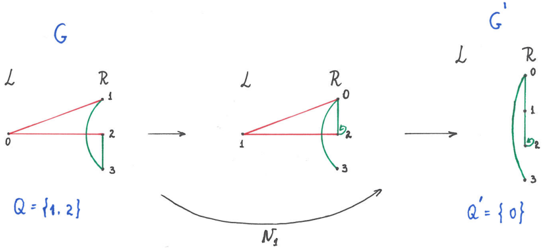
$$\begin{cases} \text{if } \mathcal{Q}_v = 1 \\ \qquad \mathcal{R}' = \mathcal{R} \setminus \{v\}, \\ \qquad G' = G + \Delta_{\{v\}}, \\ \qquad \mathcal{Q}' = \mathcal{Q} \setminus \{v\}, \\ \text{else} \\ \qquad \mathcal{R}' = \mathcal{R}, \\ \qquad (G'', \mathcal{Q}') = (G, \mathcal{Q})^v \\ \qquad G' = G'' + \Delta_{\mathcal{B}_v^G} \end{cases}, \qquad \text{if } \mathcal{B}_v^G \subset \mathcal{R}$$

Action of N on a generalised two-graph state (cont.)

Theorem (cont.)

$$\begin{cases} \text{for some } w \in \mathcal{N}_v^M, & \\ \quad (G'', \mathcal{R}'', \mathcal{Q}'') = swp(G, \mathcal{R}, \mathcal{Q}, w, v), & \\ \mathcal{R}' = \mathcal{R}'' \cup \{v\}, & \text{if } v \in \mathcal{R}, \mathcal{B}_v^G \not\subset \mathcal{R} \\ (G', \mathcal{Q}''') = (G'', \mathcal{Q}'')^v, & \\ \mathcal{Q}' = \mathcal{Q}''' \setminus \{v\}, & \end{cases}$$

Example



L_p norms

L_j-norm over every state generated by the action of the local Clifford group on $|\psi\rangle$:

$$\begin{aligned} || \, |\psi\rangle \, ||_{\mathbf{C_n},j} &= \left(192^{-n} \sum_{U \in \mathbf{C_n}} || \, |\psi_U\rangle \, ||_j^j \right)^{\frac{1}{j}} \\ &= \left(3^{-n} \sum_{U \in \{I,H,N\}^n} || \, |\psi_U\rangle \, ||_j^j \right)^{\frac{1}{j}} \\ &= 2^{\frac{n}{2}} \left(6^{-n} \sum_{\substack{\mathbf{k} \in \mathbb{Z}_2^n \\ U \in \{I,H,N\}^n}} | \, |\psi_U\rangle_{\mathbf{k}} \, |^j \right)^{\frac{1}{j}} \end{aligned}$$

L_p norms

Let $|\psi_U\rangle$ represented by $(G_U, \mathcal{R}_U, \mathcal{Q}_U)$, where $\mathcal{L}_U = \mathcal{V} \setminus \mathcal{R}_U$. Then,

$$|| \, |\psi\rangle \, ||_{\mathbf{C_n},j} = \left(3^{-n} \sum_{U \in \{I,H,N\}^n} 2^{\frac{(j-2)|\mathcal{L}_U|}{2}} \right)^{\frac{1}{j}}$$

- 192^n transforms represented by the local Clifford group $\rightarrow$ same evaluation by only 3^n transforms: $\{I, H, N\}^n$
- graph transfoms on a size n graph instead of matrix multiplication $2^n \times 2^n$
- exponential improvement in computational complexity.