Quantum Morphisms

Lecture 9

Binary Linear Systems

A binary linear system (BLS) is simply a linear system of equations over $\mathbb{Z}_2$:

$Mx = b$ s.t. $M \in \mathbb{Z}_2^{m \times n}$, $b \in \mathbb{Z}_2^m$, x a vector variable

Equation/Constraint ℓ:

$$\sum_i M_{\ell i} x_i = b_\ell \quad \text{or}$$

$$\sum_{i \in S_\ell} x_i = b_\ell \quad \text{where } S_\ell := \{ i \in [n] : M_{\ell i} = 1 \}$$

$x_1 x_2 x_3 = 1$

Example:

$$x_1 + x_2 + x_3 = 0 \qquad x_1 + x_4 + x_7 = 0$$

$$x_4 + x_5 + x_6 = 0 \qquad x_2 + x_5 + x_8 = 0$$

$$x_7 + x_8 + x_9 = 0 \qquad x_3 + x_6 + x_9 = 1$$

$x_3 x_6 x_9 = -1$

Does this system have a solution?

Mermin-Peres magic square

$$\begin{array}{c|c|c|c|l}
 & 1 & 1 & 0 & \\
\hline
1 & x_1 & x_2 & x_3 & = 0 \\
\hline
1 & x_4 & x_5 & x_6 & = 0 \\
\hline
0 & x_7 & x_8 & x_9 & = 0 \\
\hline
 & \shortparallel & \shortparallel & \shortparallel & \\
 & 0 & 0 & 1 &
\end{array}$$

$Mx = b$

M: incidence mtx of $K_{3,3}$

BLS Games

$M \in \mathbb{Z}_2^{m \times n}$, $b \in \mathbb{Z}_2^m$

(M,b)-game $\qquad f(i)=1 \iff x_i=1$

Alice sent $\ell \in [m]$, responds with $f: S_\ell \to \mathbb{Z}_2$

Bob sent $k \in [m]$, responds with $f': S_k \to \mathbb{Z}_2$

To win, they must satisfy:

$$\left.\begin{array}{l} 1)\ \sum_{i \in S_\ell} f(i) = b_\ell \\ 2)\ \sum_{j \in S_k} f'(j) = b_k \end{array}\right\} \text{– "Constraint satisfaction"}$$

3) $i \in S_\ell \cap S_k \Rightarrow f(i) = f'(i)$ "consistency"

As usual: There is a perfect classical strategy for the (M,b)-game if and only if $Mx=b$ has a solution.

Also as usual, we want a quantum analog of this.

Quantum Solutions for $Mx=b$

Multiplicative form of $Mx=b$: $1 \mapsto -1$, $0 \mapsto 1$

Variables $x_i \in \{\pm 1\}$ $\quad a \in \mathbb{Z}_2 \mapsto (-1)^a$

Equation ℓ: $\prod_{i=1}^{n} x_i^{M_{\ell i}} = (-1)^{b_\ell}$ or

$$\prod_{i \in S_\ell} x_i = (-1)^{b_\ell}$$

Relax to operator-valued variables:

A quantum solution to $Mx=b$ consists of a Hilbert space $\mathcal{H}$ and operators $A_i \in B(\mathcal{H})$ for $i \in [n]$ satisfying:

1) $A_i^* = A_i$ & $A_i^2 = I$ $\forall i \in [n]$;
2) $A_i A_j = A_j A_i$ if $\exists\, \ell \in [m]$ s.t. $i, j \in S_\ell$;
3) $\prod_{i \in S_\ell} A_i = (-1)^{b_\ell} I$ $\forall \ell \in [m]$.

Theorem (Cleve, Liu, Slofstra): The (M,b)-game has a perfect quantum commuting strategy if and only if $Mx=b$ has a quantum solution.

of forward direction

Proof Idea: "Standard techniques" show that the (M,b)-game has a perfect qc-strategy if & only if $\exists$ a C^*-algebra $\mathcal{A}$ with a tracial state and projections $P^\ell_f \in \mathcal{A}$ for $\ell \in [m]$ & $f: S_\ell \to \{\pm 1\}$ satisfying:

1) $\sum_f P^\ell_f = 1 \quad \forall\ \ell \in [m]$
2) $P^\ell_f = 0$ if $\prod_{i \in S_\ell} f(i) \neq (-1)^{b_\ell}$
3) $P^\ell_f P^k_{f'} = 0$ if $\exists\ i \in S_\ell \cap S_k$ s.t. $f(i) \neq f'(i)$

$\forall\ \ell \in [m]$ and $i \in S_\ell$ ~~$f: S_\ell \to \{\pm 1\}$~~ define:

$$A^\ell_i = \sum_{f(i)=1} P^\ell_f - \sum_{f(i)=-1} P^\ell_f = \sum_f f(i) P^\ell_f$$

Claim: $A^\ell_i = A^{\ell *}_i$, $(A^\ell_i)^2 = 1$, A^ℓ_i does not depend on ℓ

Proof of claim: $A_i^\ell = (A_i^\ell)^*$ is immediate.

$P_f^\ell P_{f'}^\ell = 0$ for $f \neq f' \Rightarrow (A_i^\ell)^2 = \sum_{f(i)=1} P_f^\ell + \sum_{f(i)=-1} P_f^\ell = \sum_f P_f^\ell = 1$

Suppose $i \in S_\ell \cap S_k$.

$$A_i^\ell A_i^k = \sum_{\substack{f: S_\ell \to \pm 1 \\ f': S_k \to \pm 1}} f(i) f'(i) \underbrace{P_f^\ell P_{f'}^k}_{=0} = \sum_{f,f'} P_f^\ell P_{f'}^k = 1$$

if $f(i) \neq f'(i)$

$\Leftrightarrow f(i) f'(i) \neq 1$

$$A_i^\ell A_i^k = 1 \Rightarrow A_i^\ell (A_i^k)^2 = A_i^k \Rightarrow A_i^\ell = A_i^k \quad \square$$

Now: $A_i := A_i^\ell$ for any ℓ s.t. $i \in S_\ell$.

Left to show:

1) $A_i A_j = A_j A_i$ if $\exists\, \ell \in [m]$ s.t. $i, j \in S_\ell$ easy
2) $\prod_{i \in S_\ell} A_i = (-1)^{b_\ell} 1$

Remarks: $A_i = P_i^+ - P_i^-$ P_f^ℓ

$\{P_i^+, P_i^-\}$ - projective measurement for just the variable x_i

A_i - called a (binary) observable

We can almost go back. Given a quantum solution $A_1, \dots, A_n \in B(\mathcal{H})$, define

$$P_i^{+1} = \tfrac{1}{2}(I + A_i) \qquad P_i^{-1} = \tfrac{1}{2}(I - A_i)$$

$$P_f^{\ell} = \prod_{i \in S_\ell} P_i^{f(i)}$$

Problem: No tracial state.

Quantum solution for Mermin-Peres magic square

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$X^* = X \qquad Y^* = Y \qquad Z^* = Z \qquad X^2 = Y^2 = Z^2 = I$$

$$XY = -YX \qquad XZ = -ZX \qquad YZ = -ZY$$

$Z \otimes I$	$I \otimes Z$	$Z \otimes Z$	I
$I \otimes X$	$X \otimes I$	$X \otimes X$	I
$Z \otimes X$	$X \otimes Z$	$Y \otimes Y$	I
I	I	$-I$	

The Solution Group

Recall the conditions of

1) $A_i^* = A_i$ & $A_i^2 = I \quad \forall i \in [n]$;
2) $A_i A_j = A_j A_i$ if $\exists\, \ell \in [m]$ s.t. $i,j \in S_\ell$;
3) $\prod_{i \in S_\ell} A_i = (-1)^{b_\ell} I \quad \forall \ell \in [m]$.

We want to encode (most of) these as group relations.

Let $M \in \mathbb{Z}_2^{m \times n}$, $b \in \mathbb{Z}_2^m$. The solution group of $Mx = b$, denoted $\Gamma(M,b)$, is the group with generators $g_1, \dots, g_n$ and J satisfying the relations:

1) $g_i^2 = e \quad \forall i \in [n]$ and $J^2 = e$;
2) $g_i J g_i^{-1} J^{-1} = e$ i.e. $g_i J = J g_i \quad \forall i \in [n]$;
3) $g_i g_j = g_j g_i$ if $\exists\, \ell \in [m]$ s.t. $i,j \in S_\ell$;
4) $\prod_{i \in S_\ell} g_i = J^{b_\ell} \quad \forall \ell \in [m]$.

Theorem (Cleve, Liu, Slofstra): Let $M \in \mathbb{Z}^{m\times n}$, $b \in \mathbb{Z}^m$.

Then the following are equivalent:

1) the (M,b)-game has a perfect qc-strategy;
2) $Mx=b$ has a quantum solution;
3) the solution group $\Gamma(M,b)$ has $J \neq e$.

"Proof": We've "seen" $(1) \Rightarrow (2)$.

$(2) \Rightarrow (3)$: A quantum solution for $Mx=b$ is a representation of the solution group where $J \mapsto -I$. But then $J \neq e$.

$(3) \Rightarrow (1)$: We show $(3) \Rightarrow (2)$ + tracial state

Let $\Gamma = \Gamma(M,b)$ and

$$\mathcal{H} = \ell^2(\Gamma) = \{ \sum_{g\in\Gamma} \alpha_g |g\rangle : \sum_g |\alpha_g|^2 < \infty \}.$$

Here $\langle g | h \rangle = \delta_{gh}$.

Define $L_g \in B(\mathcal{H})$ as $L_g|h\rangle = |gh\rangle \quad \forall g,h \in \Gamma$.

Clearly $L_g L_h = L_{gh}$.

Define $|\psi\rangle = \frac{1}{\sqrt{2}}(|e\rangle - |J\rangle)$ (unit vector since $J \neq e$)

$L_J|\psi\rangle = \frac{1}{\sqrt{2}}(|J\rangle - |e\rangle) = -|\psi\rangle$

Also $L_J L_g|\psi\rangle = L_{Jg}|\psi\rangle = L_{gJ}|\psi\rangle = L_g L_J|\psi\rangle = -L_g|\psi\rangle$.

Thus L_J acts as $-I$ on $\mathcal{H}_0 := \mathrm{span}\{L_g|\psi\rangle : g \in \Gamma\}$.

It follows that letting $A_i = L_{g_i}|_{\mathcal{H}_0} \in B(\mathcal{H}_0)$ for $i \in [n]$ gives a quantum solution for $Mx=b$.

Moreover, $A \mapsto \langle\psi|A|\psi\rangle$ is tracial on $B(\mathcal{H}_0)$ since

$$\begin{aligned}
\langle\psi|L_g L_h|\psi\rangle &= \tfrac{1}{2}\big[(\langle e| - \langle J|)(|gh\rangle - |ghJ\rangle)\big] \\
&= \tfrac{1}{2}\big[\langle e|gh\rangle + \langle J|ghJ\rangle \\
&\qquad - \langle J|gh\rangle - \langle e|ghJ\rangle\big] \\
&= \begin{cases} 1 & \text{if } gh=e \Leftrightarrow hg=e \\ -1 & \text{if } gh=J \Leftrightarrow hg=J \\ 0 & \text{o.w.} \end{cases} \\
&= \langle\psi|L_h L_g|\psi\rangle.
\end{aligned}$$

$g(hJ)=e \Rightarrow (hJ)g=e$

$Jhg=e$

$hg=J$

□

Theorem (Cleve & Mittal): Let $M \in \mathbb{Z}^{m \times n}$, $b \in \mathbb{Z}^m$.

Then the following are equivalent:

1) the (M,b)-game has a perfect quantum tensor strategy;
2) $Mx=b$ has a finite dimensional quantum solution;
3) the solution group $\Gamma(M,b)$ has a finite dimensional representation ϕ s.t. $\phi(J) \neq \phi(e)$.