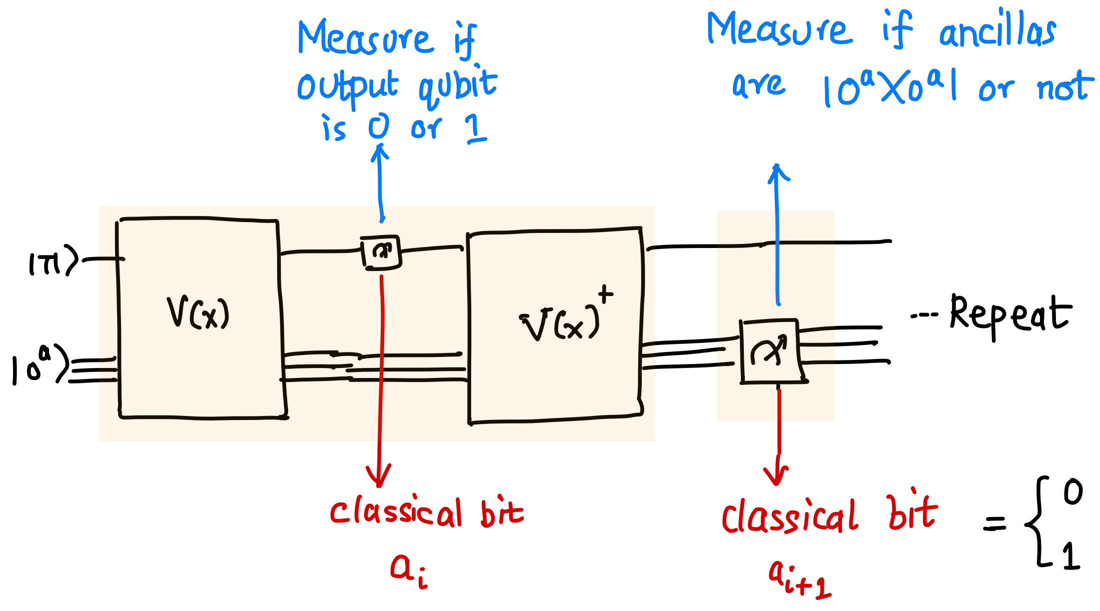
# LECTURE 15 (March 6th)

**TODAY** Witness-Preserving Error Reduction for QMA

**RECAP** Given a QMA verifier $V$ satisfying with error probability at most $1/3$ there is a new verifier $V'$ with error probability at most $2^{-\theta(n)}$ which uses the same witness as $V$

The idea is due to Marriott-Watrous who proposed the following algorithm for $V'$

①

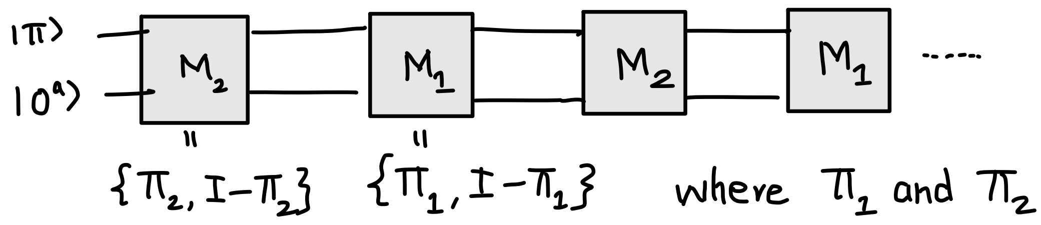

Measure if output qubit is 0 or 1
Measure if ancillas are $|0^a\rangle\langle 0^a|$ or not
$|\pi\rangle$
$|0^a\rangle$
$V(x)$
$V(x)^+$
classical bit
$a_i$
classical bit
$a_{i+1}$

--- Repeat $k = \text{poly}(n)$ times

$= \begin{cases} 0 & \text{if ancillas are } |0^a\rangle \\ 1 & \text{if not} \end{cases}$

② Compute some function of $a_1, a_2, \ldots\ldots a_k$

One can think of the above circuit $V'$ as two measurements that alternate

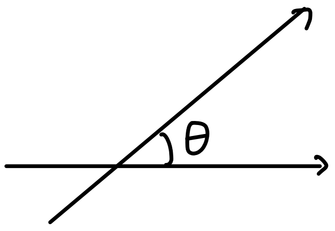


where $\Pi_1$ and $\Pi_2$ are projections on some subspaces

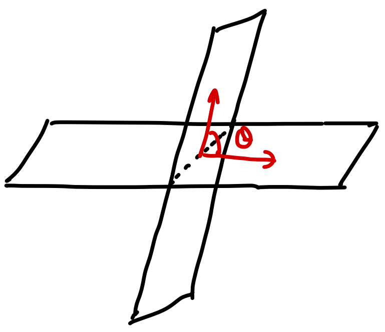
In order to analyze this, we need a technical tool called Jordan's lemma that relates to angle between two subspaces

## Angle between two subspaces

In 2-dimensions, we define angle between two lines (through origin)



In 3-dimensions, we can define angle between two planes



In 4-dimensions, we have two angles between two 2-D subspaces

Let $\Pi$ = projector on a subspace of $\mathbb{C}^d$

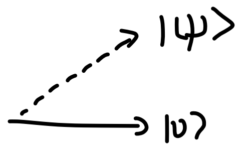
i.e. if we take a vector $|\psi\rangle$ in $\mathbb{C}^d$

$\Pi|\psi\rangle$ = projection of $|\psi\rangle$ on the subspace

Note $\Pi^2 = \Pi$, so projecting again gives the same vector

Example If $\Pi = |v\rangle\langle v|$, then $\Pi|\psi\rangle = \langle v|\psi\rangle |v\rangle$

= projection of $|\psi\rangle$ on $|v\rangle$



The question we are trying to answer:

given two projectors $\Pi_1$ & $\Pi_2$, how do they interact?

**Jordan's Lemma**

Proof in lecture notes

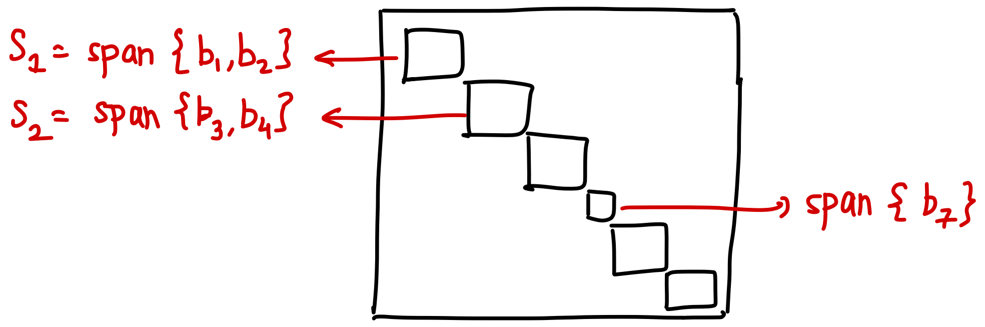
For any two projectors $\Pi_1$ and $\Pi_2$ in $\mathbb{C}^d$

There exist a decomposition of $\mathbb{C}^d$ into orthogonal 1- & 2-dimensional subspaces that are invariant under both $\Pi_1$ & $\Pi_2$

Moreover, inside each of these two-dimensional subspaces $\Pi_1$ and $\Pi_2$ are rank one projectors

$\{b_1, \ldots, b_d\}$

Or in other words, there is some basis s.t. both $\Pi_1$ & $\Pi_2$ look simultaneously block-diagonal in this basis & moreover each block is of size atmost 2.



$S_1 = \text{span}\{b_1, b_2\}$

$S_2 = \text{span}\{b_3, b_4\}$

span $\{b_7\}$

For any vector $|v\rangle$ in $S_i$,

$\Pi_1|v\rangle \in S_i$

$\Pi_2|v\rangle \in S_i$

Moreover, $\Pi_1$ when restricted to $S_i$

$$\Pi_1|_{S_i} = |v_i\rangle\langle v_i| \quad \text{for some } |v_i\rangle \in S_i$$

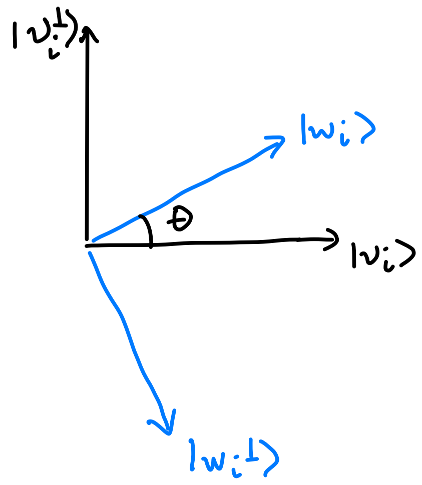
Similarly,

$$\Pi_2|_{S_i} = |w_i\rangle\langle w_i| \quad \text{for some } |w_i\rangle \in S_i$$

One can define angles $\theta_i := \cos^{-1}(|\langle v_i|w_i\rangle|)$ as the principal angles between the subspaces

$\in$
$[0, \frac{\pi}{2}]$

$S_i = \text{span}\{|v_i\rangle, |v_i^\perp\rangle\} = \text{span}\{|w_i\rangle, |w_i^\perp\rangle\}$ for some vectors $|v_i^\perp\rangle$ & $|w_i^\perp\rangle$ orthogonal to $|v_i\rangle$ & $|w_i\rangle$ respectively



Let $p_i = \cos^2\theta_i = |\langle v_i|w_i\rangle|^2$

The lemma easily allow us to understand what happens in we apply $\pi_1\pi_2\pi_1$

It is clearly block-diagonal in the Jordan decomposition and inside each $S_i$

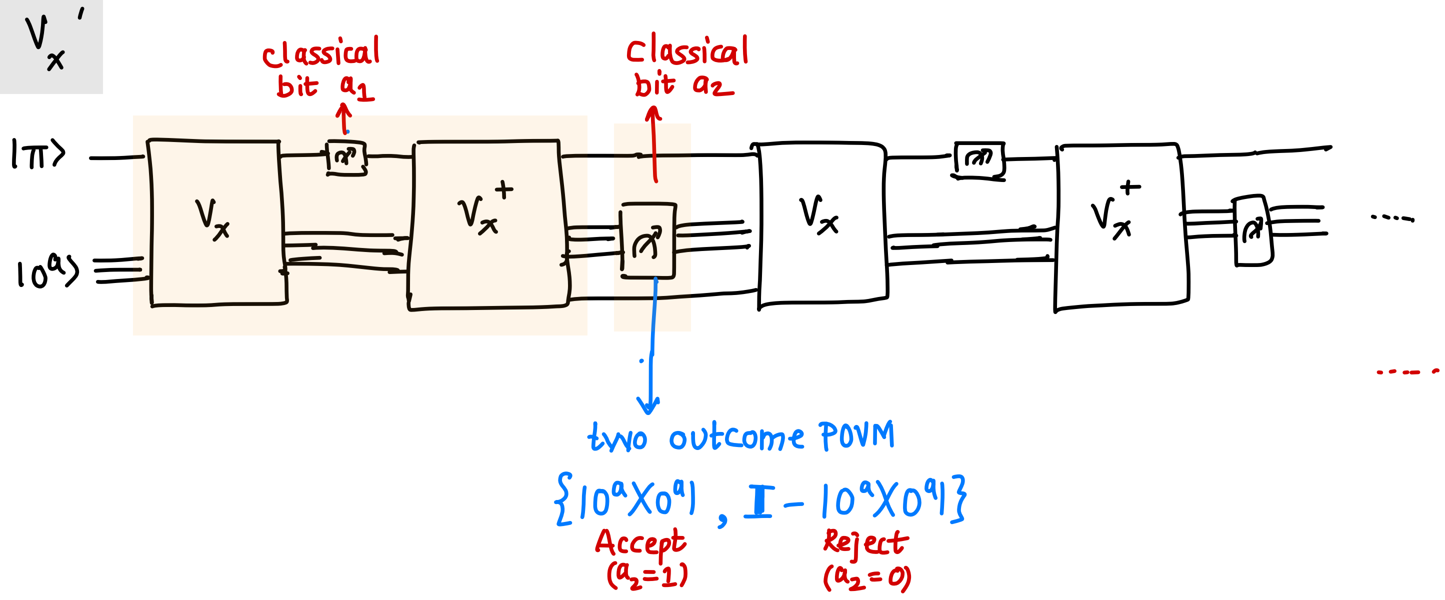
$$\Pi_1\Pi_2\Pi_1|_{S_i} = |v_i\rangle\underbrace{\langle v_i||w_i\rangle}_{}\underbrace{\langle w_i||v_i\rangle}_{}\langle v_i| = p_i\, |v_i\rangle\langle v_i|$$

Mariott- Watrous Amplification Let $V_x$ be the QMA verifier with error $\leq \frac{1}{3}$

We can assume that $\forall$ proof $|\pi\rangle$, $\mathbb{P}[\, V_x$ accepts $|\pi\rangle\,] \in (0,1)$

New verifier $V_x'$

①



② Accept if $a_i = a_{i+1}$ for at least half the indices $i$

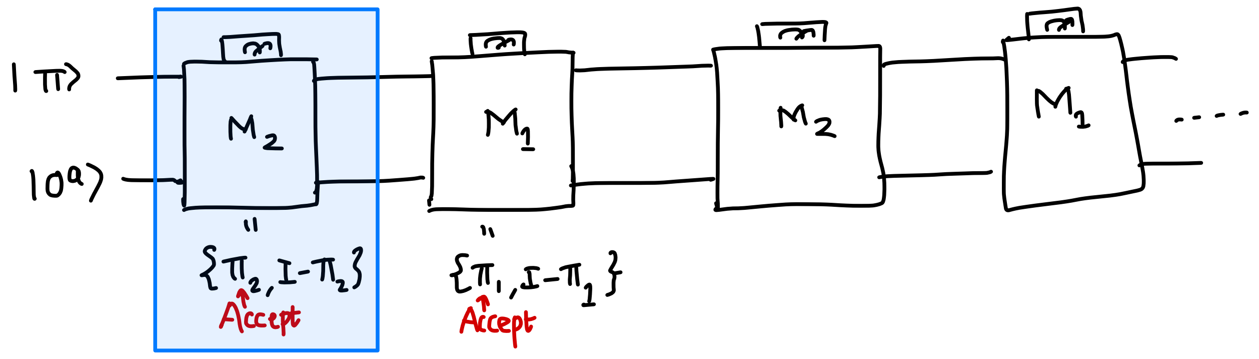
Claim If $x \in L \Rightarrow \exists |\pi\rangle$, $V_x'$ accepts w.p. $\geq 1 - 2^{-\Theta(n)}$

If $x \notin L \Rightarrow \forall |\pi\rangle$, $V_x'$ accepts w.p. $\leq 2^{-\Theta(n)}$

Proof To apply Jordan's lemma, consider the two projectors

$$\Pi_1 = \underbrace{|0^a\rangle\langle 0^a|}_{\text{auxillary qubits are all zeros}} \otimes I \quad \& \quad \Pi_2 = \overset{\text{original QMA verifier with } \frac{1}{3} \text{ error}}{V_x^{+}\big(\underbrace{|0\rangle\langle 0|}_{\text{output qubit is 0}} \otimes I\big) V_x}$$

Then, the circuit is



↳ This is the original verifier $V_x$ with 2/3 success probability

Note that acceptance probability of QMA verifier $V_x$ = max eigenvalue of $\Pi_1\Pi_2\Pi_1$

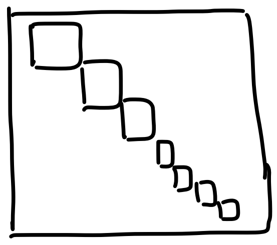
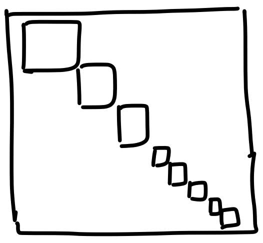
$\Pi_1$ just restricts the initial states to the form $|\pi\rangle \otimes |0^a\rangle$

We now apply Jordan's lemma to obtain 2-dimensional subspaces $S_1, S_2, \ldots$ and 1-dimensional subspaces $T_1, T_2, \ldots$

and $\Pi_1|_{S_i} = |v_i\rangle\langle v_i|$

$\Pi_2|_{S_i} = |w_i\rangle\langle w_i|$ and $p_i = |\langle v_i|w_i\rangle|^2$

Pictorially,

$\Pi_1 =$  $\Pi_2 =$ 

We claim that all the one dimensional blocks of $\Pi_1$ are zero otherwise we could choose a witness in $T_i$ and achieve success probability 0 or 1 which contradicts our assumption

So, we can focus on the two dimensional subspaces $S_i$'s

As we have seen previously,

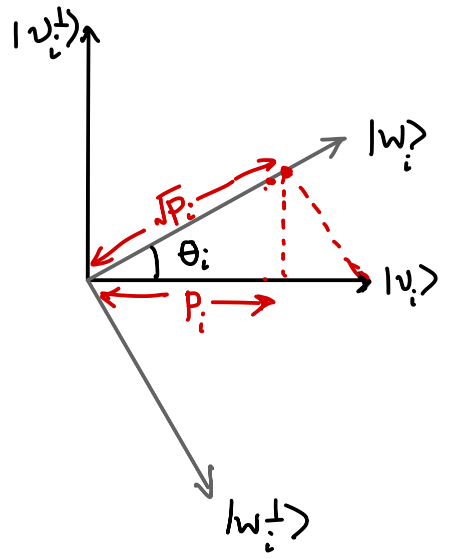
$$\Pi_1\Pi_2\Pi_1 = \sum_i p_i |v_i\rangle\langle v_i|$$

Thus, max eigenvalue of $\Pi_1\Pi_2\Pi_1$ = maximum acceptance prob. of $V_x$ = $\max_i p_i$

## Analysis of new Verifier $V'_\pi$

Let us analyze what happens when we give us input a vector $|\psi\rangle$ in the 2-dimensional subspace $S_i = \text{span}\{|v_i\rangle, |v_i^\perp\rangle\} = \text{span}\{|w_i\rangle, |w_i^\perp\rangle\}$

Recall that $\Pi_{1|S_i} = |v_i\rangle\langle v_i|$ and $\Pi_{2|S_i} = |w_i\rangle\langle w_i|$ and applying either one we remain in the subspace $S_i$



Let us look at the case when input $= |v_i\rangle$ and we apply $M_2$ first and then $M_2$

After applying $M_{2|S_i} = \{|w_i\rangle\langle w_i|, |w_i^\perp\rangle\langle w_i^\perp|\}$

$$\begin{tikzcd}
|v_i\rangle \arrow[r, "p_i"] \arrow[dr, "1-p_i"'] & |w_i\rangle \arrow[r] & \text{Accept state } (a_i\text{'s} = 1) \\
& |w_i^\perp\rangle \arrow[r] & \text{Reject state } (a_i\text{'s} = 0)
\end{tikzcd}$$

probabilities    post-measurement state

After applying $M_{1|S_i} = \{|v_i\rangle\langle v_i|, |v_i^\perp\rangle\langle v_i^\perp|\}$

$$\begin{tikzcd}
|w_i\rangle \arrow[r, "p_i"] \arrow[dr, "1-p_i"] & |v_i\rangle \arrow[r] & \text{Accept state } (a_i\text{'s} = 1) \\
|w_i^\perp\rangle \arrow[r, "p_i"'] \arrow[ur] & |v_i^\perp\rangle \arrow[r] & \text{Reject state } (a_i\text{'s} = 0)
\end{tikzcd}$$

probabilities    post-measurement state

Overall, if starting state was either $|v_i\rangle$ or $|v_i^\perp\rangle$, we get

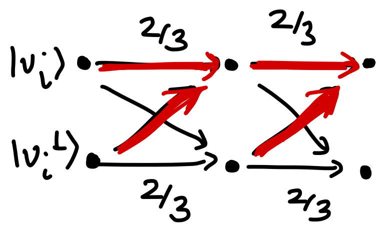
$$\begin{tikzcd}
|v_i\rangle \arrow[r, "p_i"] \arrow[dr] & |w_i\rangle \arrow[r, "p_i"] \arrow[dr] & |v_i\rangle & \cdots \\
|v_i^\perp\rangle \arrow[r, "p_i"'] \arrow[ur] & |w_i^\perp\rangle \arrow[r, "p_i"'] \arrow[ur] & |v_i^\perp\rangle &
\end{tikzcd}$$

Red edges correspond to "Accept" or "1" outcome

So, keep alterating between these four states by applying $M_1$ & $M_2$

Now, if $x \in L$, we know that $p_i \geqslant 2/3$ for some $i$ and we provide $|v_i\rangle$ as witness

So, picture looks like



Suppose we start from $|v_i\rangle$

$\mathbb{P}$[ Obtaining $\underset{\rightarrow\rightarrow}{\text{"11"}}$ or $\underset{\searrow\rightarrow}{\text{"00"}}$ ] $\geqslant 2/3$

So, if we do $k$ iterations, atleast $2/3\, k$ of the times $a_i = a_{i+1}$ in expectation

$\Rightarrow$ success probability is $\geqslant 1 - 2^{-\Theta(n)}$

If $x \notin L$ We want to show $\forall\, |\psi\rangle$ with all ancilla bits zero (i.e. $|\psi\rangle$ is in the subspace on which $\Pi_1$ projects)

Note that this subspace is spanned by $|v_1\rangle, |v_2\rangle, \ldots$

$V_x'$ accepts with probability $\leq 2^{-\Theta(n)}$

If $|\psi\rangle = |v_i\rangle$, then the probabilities of red and black edges get switched and the proof follows

Otherwise, one can write $|\psi\rangle = \sum \alpha_i |v_i\rangle$ and show that probability of "11" or "00" is still atmost $\leq \frac{1}{3}$, no matter the current state

## One Application of Witness-preserving Amplification

Classically we know that $NP_{\log} = P$ where $NP_{\log}$ denotes the complexity class where witnesses are $O(\log \text{input-size})$

Witness preserving amplification allows one to show a similar characterization for QMA

$$QMA_{\log} = BQP$$

You will be asked to show this in the exercises. The proof relies on the fact that witness size does not increase (too much)

NEXT TIME Complete Problems for QMA

Proof of Jordan's Lemma

Consider the matrix $\Pi_1 + \Pi_2$

This is a Hermititian matrix and can be spectrally decomposed

$$\Pi_1 + \Pi_2 = \Sigma \lambda_i |v_i\rangle\langle v_i|$$

We shall show that $\{|v_i\rangle\}$'s can be partitioned into sets of size one and two where each set spans an invariant subspace

Take an eigenvector $|v_i\rangle$ : then $\Pi_1|v_i\rangle + \Pi_2|v_i\rangle = \lambda_i|v_i\rangle$

① If $\Pi_1|v_i\rangle \in \text{span}(|v_i\rangle)$, then so is $\Pi_2|v_i\rangle$

This gives a one-dimensional invariant subspace span $\{|v_i\rangle\}$

Note $\Pi_1|v_i\rangle = |v_i\rangle$ or $\Pi_1|v_i\rangle = 0$

and same for $\Pi_2$

② If $\Pi_1|v_i\rangle \notin \text{span}(|v_i\rangle)$, consider the 2-dimensional subspace

$$S = \text{span}\{|v_i\rangle, \Pi_1|v_i\rangle\}$$

This is an invariant subspace for $\Pi_1$ since

$$\Pi_1(\alpha|v_i\rangle + \beta\Pi_1|v_i\rangle) = \alpha\Pi_1|v_i\rangle + \beta\Pi_1^2|v_i\rangle = (\alpha+\beta)\Pi_1|v_i\rangle \in S$$

It is also invariant for $\Pi_2$ since

$$\Pi_2(\alpha|v_i\rangle + \beta\Pi_1|v_i\rangle) = \alpha\underbrace{\Pi_2|v_i\rangle}_{=\lambda_i|v_i\rangle - \Pi_1|v_i\rangle} + \beta\Pi_2\overbrace{\Pi_1|v_i\rangle}^{=\lambda_i|v_i\rangle - \Pi_2|v_i\rangle}$$

$$= \alpha\Pi_2|v_i\rangle + \beta\Pi_2(\lambda_i|v_i\rangle - \Pi_2|v_i\rangle)$$

$$= (\alpha + \beta\lambda_i - \beta)\underbrace{\Pi_2|v_i\rangle}_{\in S}$$

Since $\Pi_1$ and $\Pi_2$ are both invariant for $S$, so is $\Pi_1 + \Pi_2$

The vector orthogonal to $|v_i\rangle$ in $S$ is also some other eigenvector $|v_j\rangle$

It is also easy to check that $\Pi_1$ and $\Pi_2$ are rank-one projectors when restricted to $S$ □