evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Kvantové hrebene –

formalizmus všeobecných kvantových protokolov

Michal Sedlák

Fyzikálny Ústav SAV

Bratislava

Spolupracovníci z Pávie: **Prof. G.M. D'Ariano, P. Perinotti, A. Bisio**

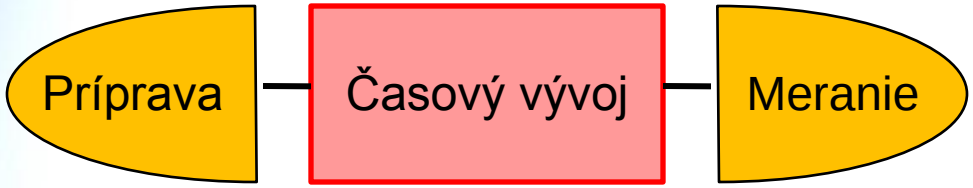
Školiteľ počas PhD: **Prof. Vladimír Bužek**

Spolupracovníci počas PhD: **M. Ziman, M. Hillery**

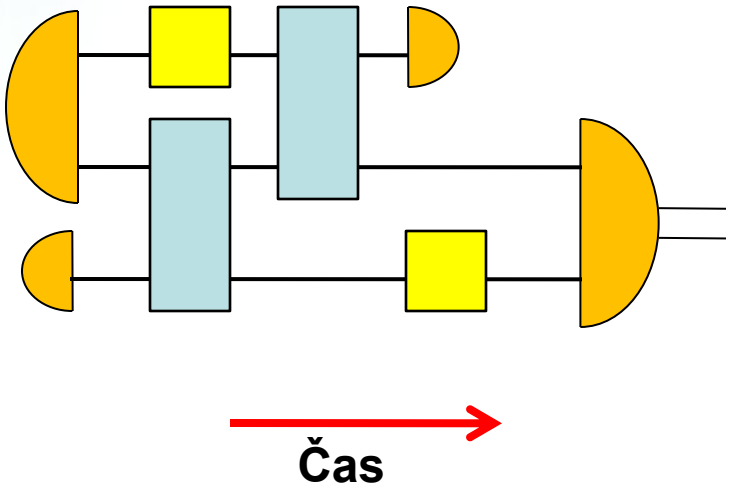
20.3.2012, Univerzita Palackého v Olomouci

Kvantový obvod

- Schéma ľubovoľného kvantového experimentu
- skladá sa z troch druhov objektov:



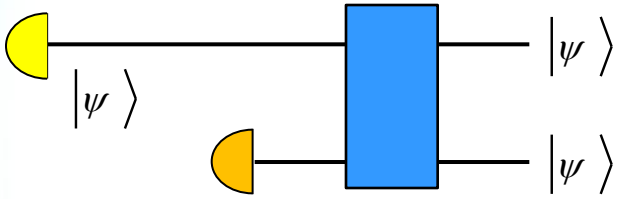
- vodorovné čiary znázorňujú vstup/výstup kvantových systémov
- Opakovanie tej istej udalosti = viacnásobný výskyt daného symbolu v schéme



Optimalizácia kvantových protokolov

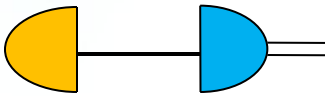
Protokol = ľubovoľný postup na dosiahnutie stanovenej úlohy

Klonovanie



Optimalizujeme transformáciu

Rozlišovanie stavov

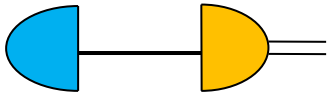


Optimalizujeme meranie

Optimalizácia kvantových protokolov

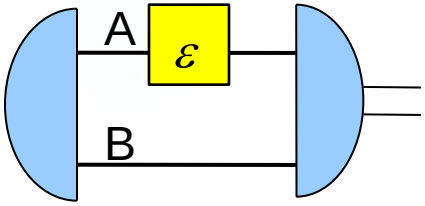
Protokol = ľubovoľný postup na dosiahnutie stanovenej úlohy

Informačná sila merania



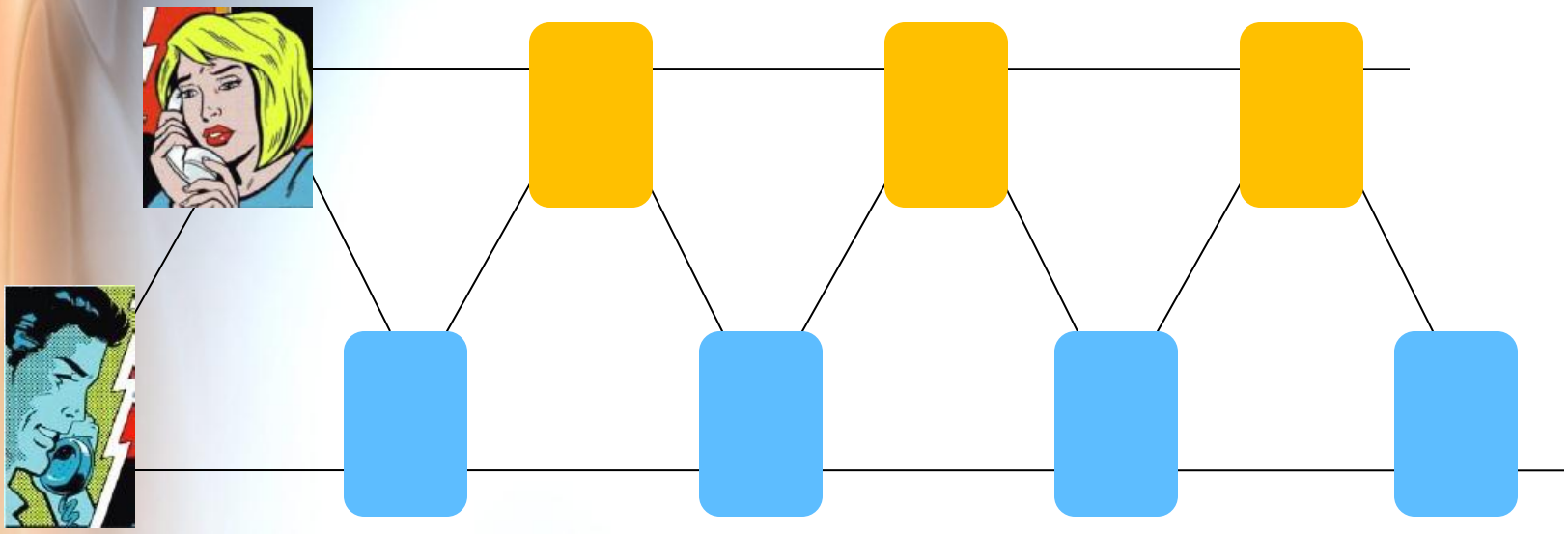
Optimalizujeme
Vstupné stavy

Odhad/rozlišovanie transformácii

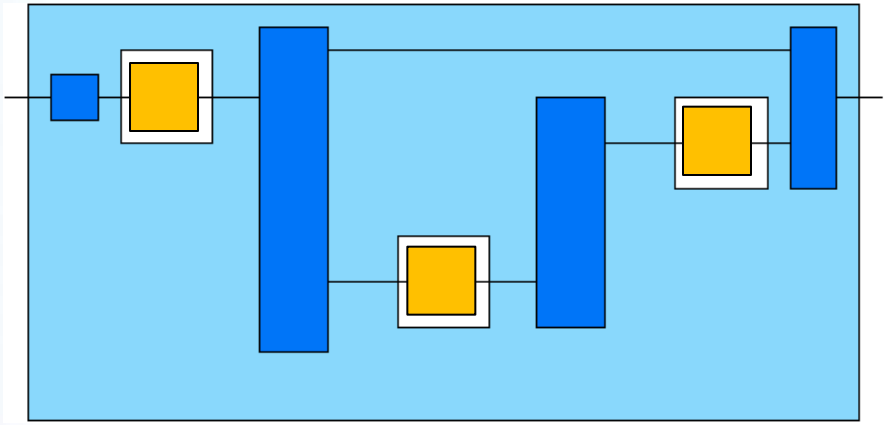


Optimalizujeme
viaceré súčasti
kvantového obvodu

Viackolová interakcia dvoch entít



Kvantové algoritmy volajúce orákulá



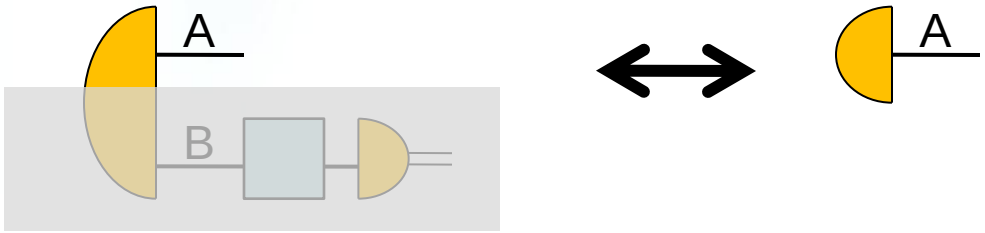
Matice hustoty a viaccasťové kvantové systémy

- množina stavov kvantového systému s Hilbertovým priestorom H_A

$$\rho \geq 0, \quad Tr(\rho) = 1, \quad \rho \in L(H_A)$$

- **čisté stavy** $Tr(\rho^2) = 1$ $\quad \rho = |\psi\rangle\langle\psi|$

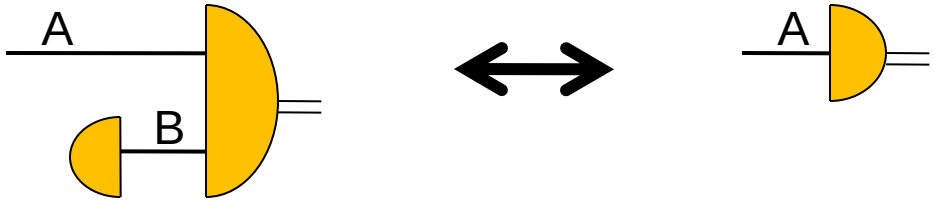
- Dva systémy s Hilbertovými priestormi H_A, H_B môžu byť v stavoch $\rho \in L(H_A \otimes H_B)$



- Stav podsystému A: $\rho_A = Tr_B(\rho)$

POVM merania

- Každé meranie možno chápať ako projektívne meranie na väčšom systéme



- Namiesto popisu merania pomocou ON bázy máme pozitívne operátory

$$E_i \geq 0 \qquad \sum_{i=1}^{N} E_i = \mathbf{1}$$

$$p(i) = Tr(\rho E_i)$$

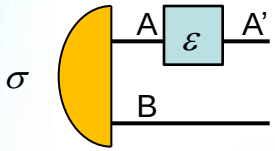
Typické využitie:

- Optimalizácie meraní pre estimácie a rozlišovanie stavov
- Pohodlná parametrizácia dosiahnuteľných pravdepodobnostných distribúcii na stavoch

Kvantové kanály

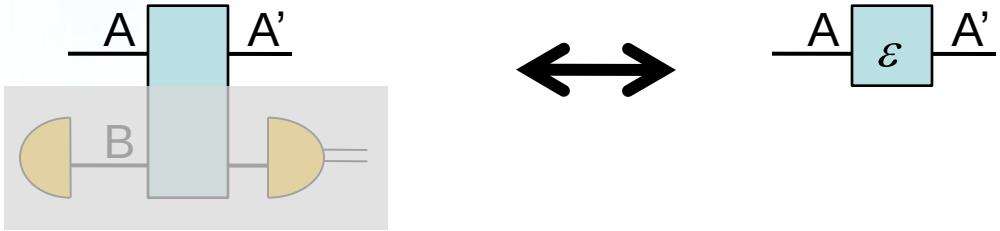
- Najvšeobecnejší možný časový vývoj systému A
- Lineárne, **úplne pozitívne** a stopu zachovávajúce zobrazenie na $L(\mathcal{H}_A)$

$\varepsilon(\rho) \geq 0$ Pozitivita



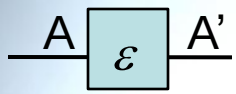
$\varepsilon \otimes I(\sigma) \geq 0$ **Úplná pozitivita**

- Každý časový vývoj systému A možno interpretovať ako unitárny vývoj na väčšom systéme (Stinespring)



- Krausova reprezentácia

$$\varepsilon(\rho) = \sum_i K_i \rho K_i^+ \qquad \sum_i K_i^+ K_i = \mathbf{1}$$



Kvantové kanály

- vhodný na popis množiny kanálov je CHOI-JAMIOLKOWSKI izomorfizmus

$$E = \varepsilon \otimes I\left(\left|\Omega\right\rangle\left\langle\Omega\right|\right) = \sum_{i,j} \varepsilon\left(\left|i\right\rangle\left\langle j\right|\right) \otimes \left|i\right\rangle\left\langle j\right| \qquad \left|\Omega\right\rangle \equiv \sum_{i=1}^{d} \left|i\right\rangle\left|i\right\rangle \in H_A \otimes H_A \qquad E \in L\left(H_{A'} \otimes H_A\right)$$

- Aplikácia kanálu na vstupný stav sa z Choi matice získa ako

$$\varepsilon\left(\rho\right) = Tr_A\left(E\ \mathbf{1} \otimes \rho^T\right)$$

- Úplnú pozitívnosť a zachovávanie stopy zabezpečujú podmienky

$$E \geq 0 \qquad Tr_{A'}\left(E\right) = \mathbf{1}_A$$

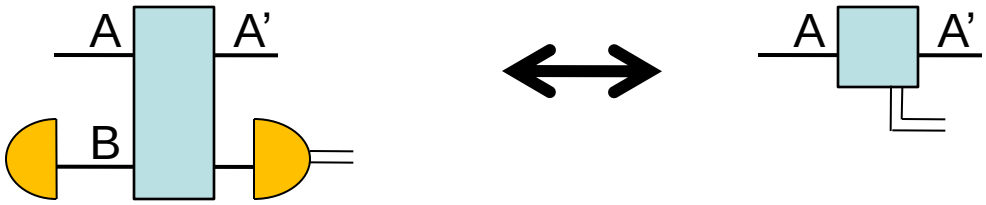
- Súvis s minimálnou Krausovou reprezentáciou

$$E = \sum_i \left|K_i\right\rangle\left\langle K_i\right| \qquad \left|K_i\right\rangle \equiv K_i \otimes \mathbf{1}\left|\Omega\right\rangle$$

Kvantové inštrumenty

= merania s klasickým aj kvantovým výstupom

Každý inštrument je dosiahnuteľný ako unitárny vývoj na väčšom systéme nasledovaný meraním na ancile



- v CHOI-JAMIOLKOWSKI izomorfizme

$$E_i \geq 0 \qquad Tr_{A'}\left(\sum_i E_i\right) = \mathbf{1}_A$$

- Ignorovanie klasického výsledku inštrumentu vedie ku kanálu

$$E = \sum_i E_i$$

Na čo sú kanály medzi rôznymi priestormi?

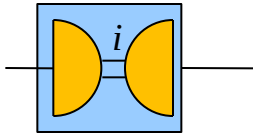
Všetky zariadenia možno chápať ako kanály

Zavedieme 1-rozmerný Hilbertov priestor $H_{\varnothing}$ s bázou $|e_{\varnothing}\rangle$

$$A \in L(H_X) \quad \longleftrightarrow \quad A \otimes |e_{\varnothing}\rangle\langle e_{\varnothing}| \in L(H_X \otimes H_{\varnothing})$$

Stav $\rho \in L(H_A)$ **=** **kanál** z 1-rozmerného Hilbertovho priestoru $H_{\varnothing}$ do H_A

POVM $\{E_i\}_{i=1}^{N}$ na H_A **=** **kanál** z H_A do $\square_N$, pričom výsledok i sa kóduje do ON stavov



$$\mathcal{E}(\rho) = \sum_i |i\rangle\langle i| \; Tr(\rho E_i)$$

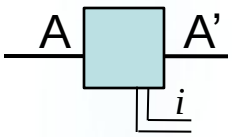
Na čo sú kanály medzi rôznymi priestormi?

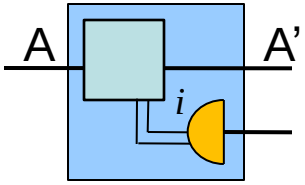
Všetky zariadenia možno chápať ako kanály

Inštrument = **kanál** z H_A do $H_{A'} \otimes$ □ $_N$

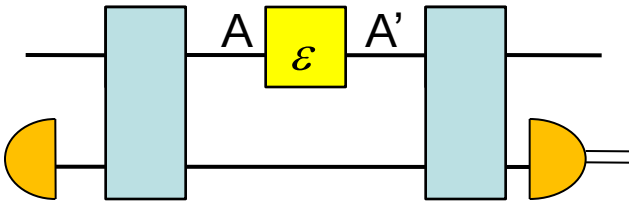
$$\{E_i\}_{i=1}^{N} \subset L(H_{A'} \otimes H_A)$$

výsledok i sa kóduje do ON stavov





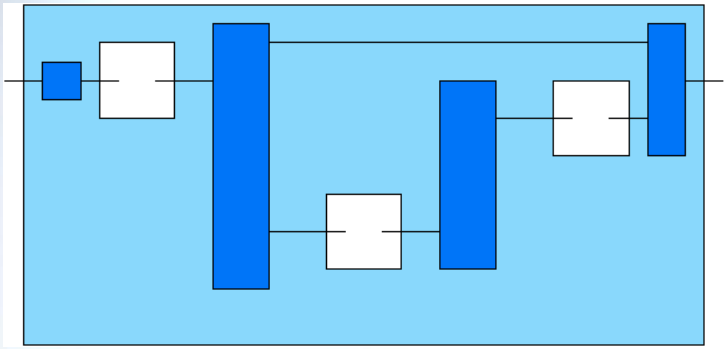
Ako charakterizovať transformácie kvantových kanálov?



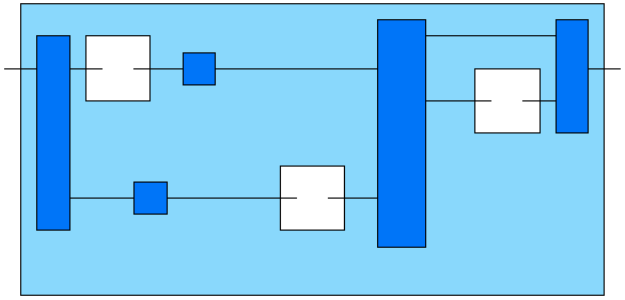
- Chceme nájsť popis, ktorý bude nezávislý na implementácii

Neúplné kvantové obvody

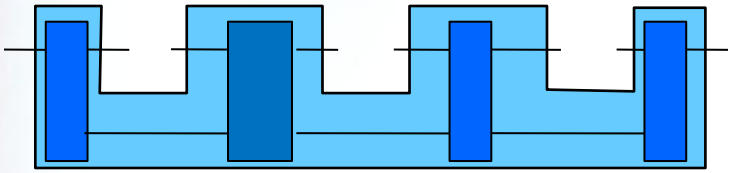
- **Kvantové obvody s „dierami“**

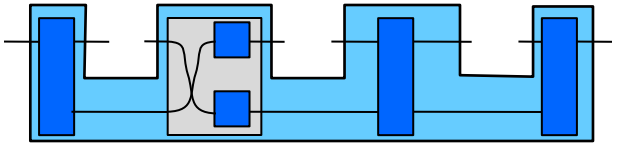


- Viaceré obvody robia rovnakú vstupno-výstupnú transformáciu



- Preusporiadaním drôtov sú zakresliteľné v tvare hrebeňa

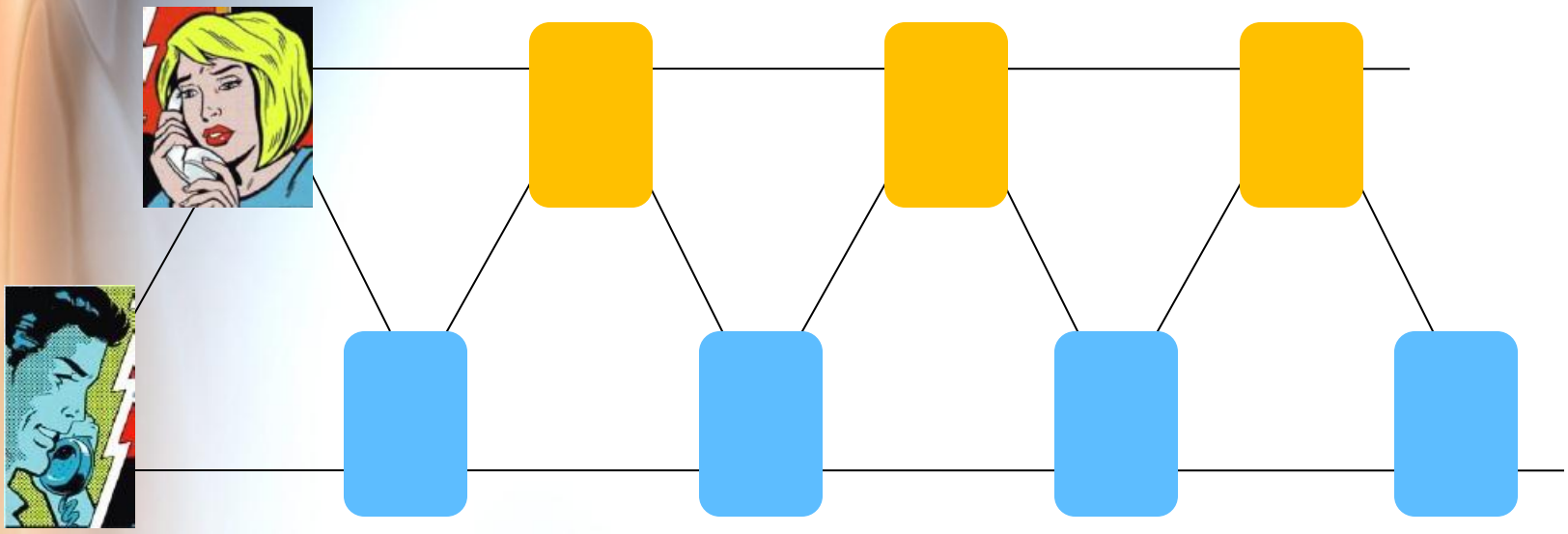




Objekt záujmu = triedy neúplných kvantových obvodov

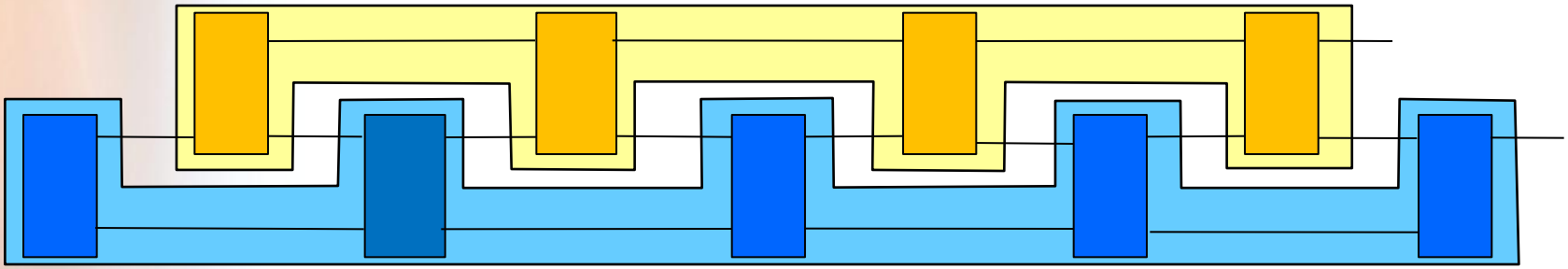
Najvhodnejší matematický formalizmus = **Kvantové hrebene**

Viackolová interakcia dvoch entít

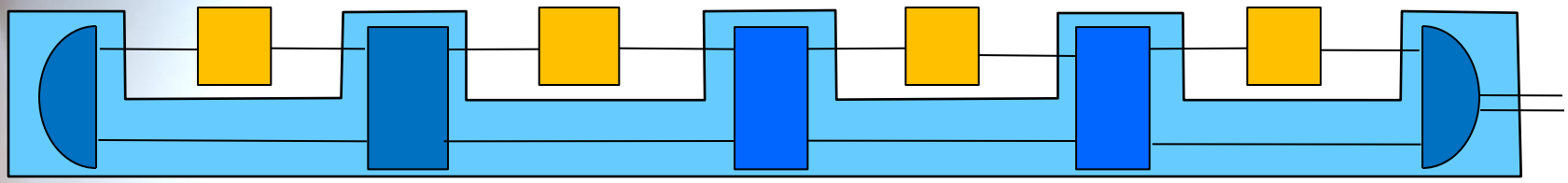


Vhodný formalizmus

- **Kvantové hrebene**

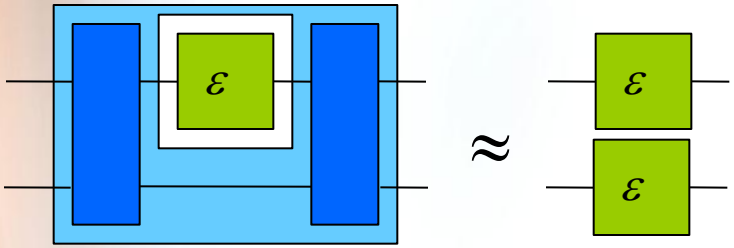


Kvantové algoritmy volajúce orákulá



- Príkladom je hľadanie v neusporiadanej databáze

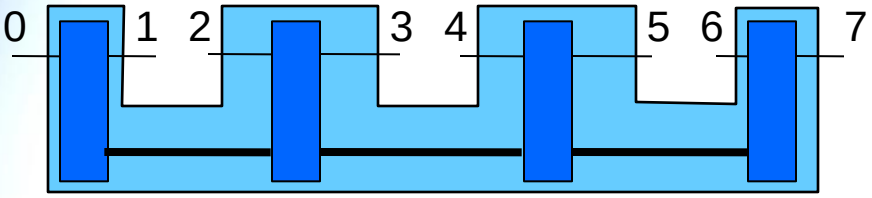
Optimálne stratégie pre zvolenú úlohu



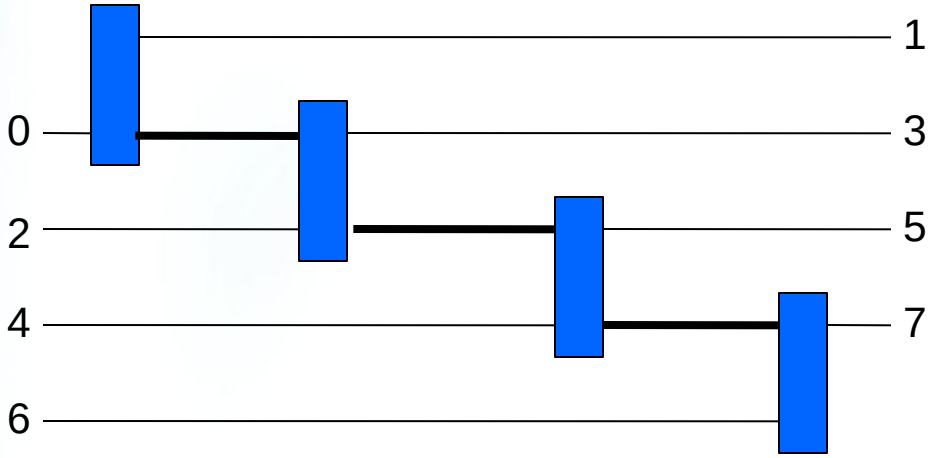
Príklad:

- Klonovanie kvantových kanálov

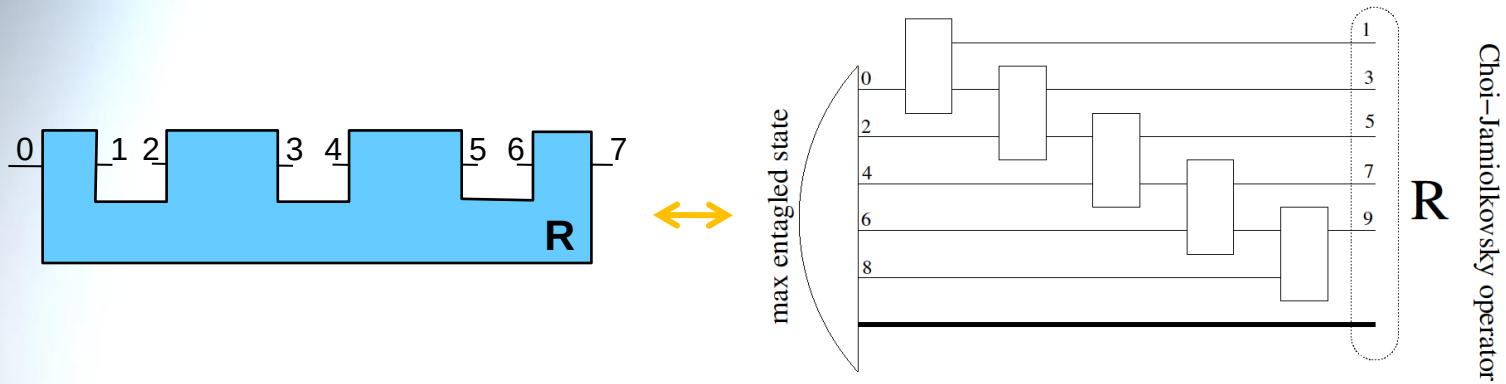
Neúplný kvantový obvod = pamäťový kanál



- Každý kvantový obvod má štruktúru pamäťového kanála



Kvantový hrebeň



Kvantový hrebeň = Choi operátor R pamäťového kanálu

- Reprezentuje triedu ekvivalencie neúplných kvantových obvodov

Kauzálna štruktúra kvantového hrebeňa vedie k normalizácii:

$$Tr_{2n-1}\left(R^{(n)}\right) = \mathbf{1}_{2n-2} \otimes R^{(n-1)} \qquad \forall\, n = 2, \cdots, N \qquad R^{(N)} \equiv R$$

$$Tr_{1}\left(R^{(1)}\right) = 1$$

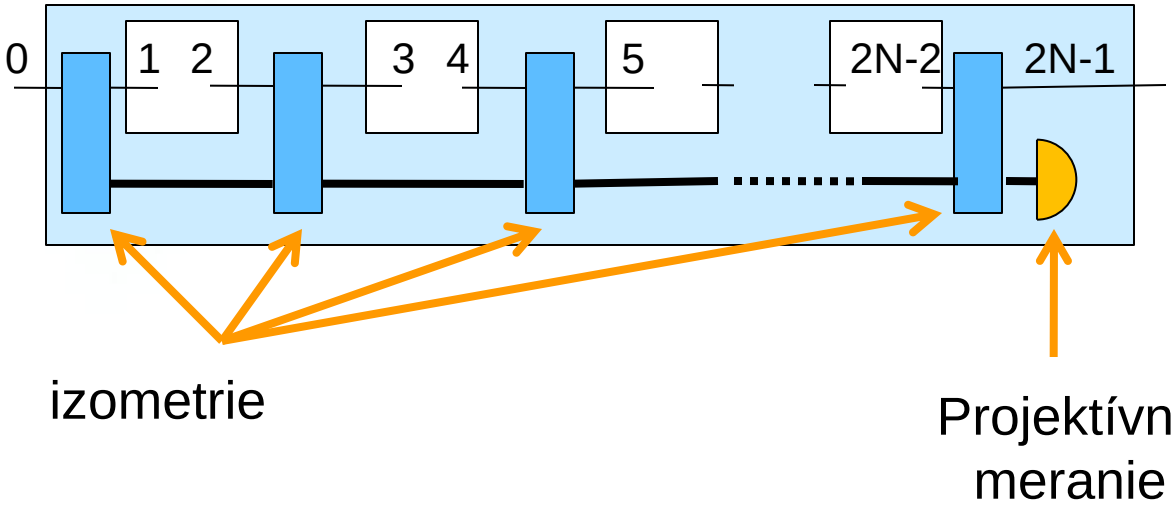
Kvantový hrebeň – realizačná teoréma

Pre každé R spĺňajúce normalizáciu

$$Tr_{2n-1}\left(R^{(n)}\right) = \mathbf{1}_{2n-2} \otimes R^{(n-1)} \qquad \forall n = 2,\cdots,N \qquad R^{(N)} \equiv R$$

$$Tr_{1}\left(R^{(1)}\right) = 1$$

Existuje kvantový obvod nasledujúceho tvaru, ktorý ho realizuje

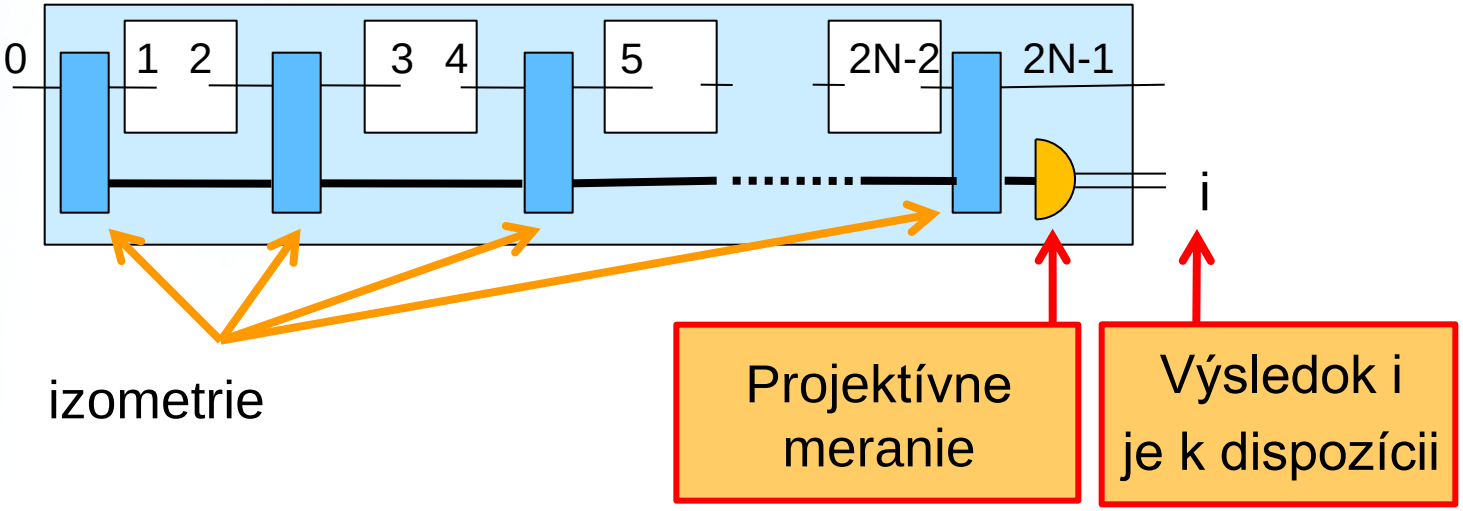


Zovšeobecnený kvantový inštrument

Pre každú sadu pozitívnych operátorov, ktoré sa sumujú do kvantového hrebeňa

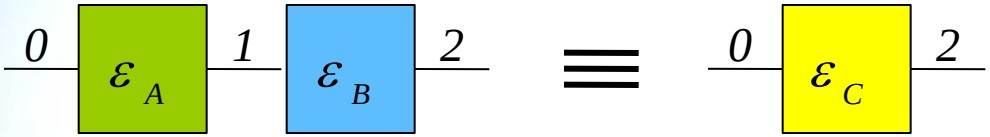
$$\{R_i\}_{i=1}^{M}, \qquad R_i \geq 0, \qquad \sum_{i=1}^{M} R_i \equiv R^{(N)}$$

Existuje kvantový obvod s nasledovnou štruktúrou, ktorý ho realizuje



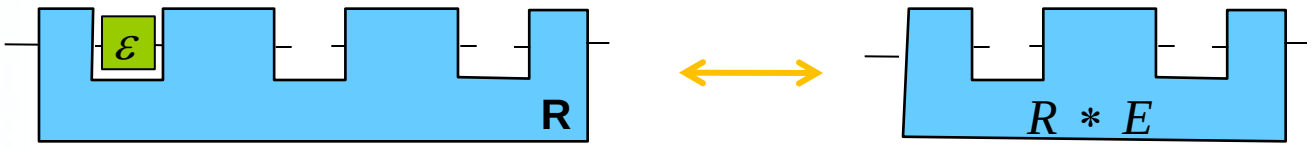
Hviezdičkový súčin – spájanie vstupov s výstupmi

Sekvenčná kompozícia kanálov motivuje definíciu **hviezdičkového súčinu ich Choi matíc**

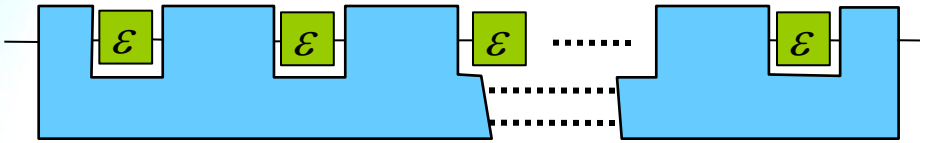


$$E_A * E_B \equiv E_C = Tr_1\left(E_A \otimes \mathbf{1}_2.\mathbf{1}_0 \otimes E_B^{T_1}\right)$$

Vloženie kanálu do hrebeňa zodpovedá hviezdičkovému súčinu



Optimalizačné úlohy s N použitiami kanálu

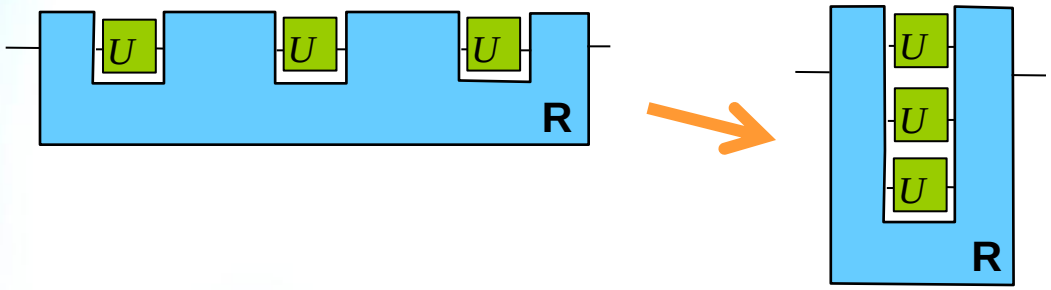


- Každá úloha s obmedzenými zdrojmi je formulovateľná ako optimalizácia kvantového hrebeňa / zovšeobec-neného inštrumentu vzhľadom na istú cost-funkciu
- Množina hrebeňov / inštrumentov je konvexná
- Realizačná teoréma poskytuje najmenšie pomocné kvantové systémy potrebné pre obvody obsahujúce merania až v poslednom kroku
- Izometrie môžeme rozložiť do elementárnych kvantových brán (1 a 2 qubitových transformácii)

Výsledky hrebeňov pre unitárne kanály

Cost funkcia má symetriu => hľadáme symetrický hrebeň

Symetria hrebeňa => paralelizovateľnosť použití kanála

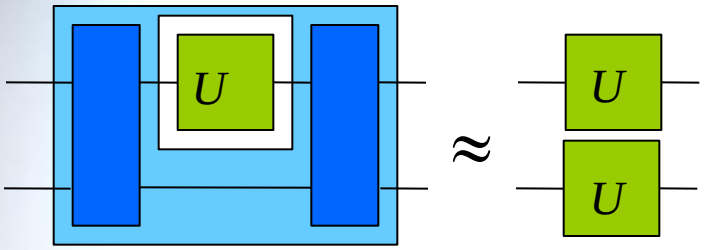


Optimálne kvantové obvody boli nájdené pre:

- Estimáciu kanála z N použití
- Klonovanie unitárneho kanála z 1 použitia na 2
- Learning unitárneho kanála z N použití
- Invertovanie neznámeho unitárneho kanála
- Vzťah medzi informatívnosťou estimácie a narušením unitárnej transformácie

Klonovanie unitárneho kanála 1→2

Cost funkcia je priemerná hodnota tzv. Channel Fidelity

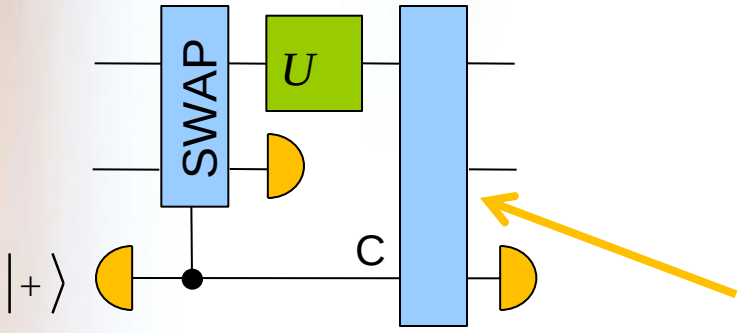


$$F = \frac{1}{d^4} \int_{U(d)} dU \; Tr\left[E_U \otimes E_U \left(R * E_U \right) \right]$$

$$E_U = \left| U \right\rangle\!\rangle \langle\!\langle U \right| \qquad \left| U \right\rangle\!\rangle = U \otimes \mathbf{1} \sum_i \left| i \right\rangle \left| i \right\rangle$$

Optimálne klonovanie:

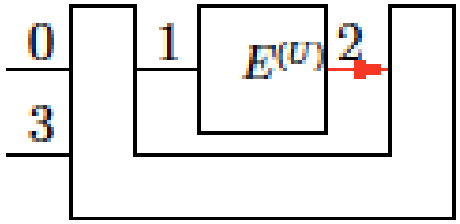
$$F = \frac{\left(\sqrt{d_+} + \sqrt{d_-} \right)^2}{d^4}$$



Optimálne klonovanie stavov ak je vstup C v $\left| + \right\rangle = \frac{1}{\sqrt{2}} \left(\left| 0 \right\rangle + \left| 1 \right\rangle \right)$

G. Chiribella, G. M. D'Ariano, P. Perinotti, Phys. Rev. Lett. 101, 180504 (2008)

Optimálne klonovanie POVM 1→2



- Obmedzíme sa na Von Neumannové merania, ktoré reprezentujeme kanálom

$\{|i\rangle\}_{i=1}^{d}$ - ON báza

$$E_i^{(U)} = U\,|i\rangle\langle i|\,U^{\dagger} \qquad E = \sum_{i=1}^{N} |i\rangle\langle i|_{out} \otimes E_i^{T}$$

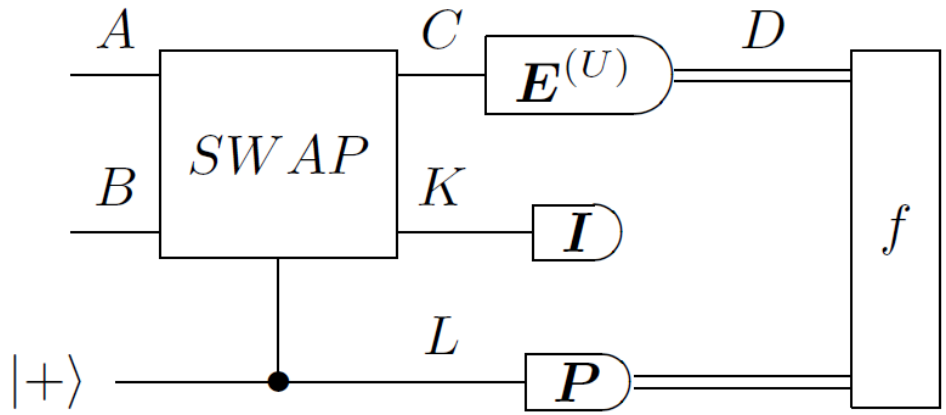
- Predpokladáme rovnomernú pravdepodobnosť ich výskytu

Cost funkcia:

- Priemerná „blízkosť“ klonovaného a originálneho POVM

$$F = \int_{SU(d)} dU \, \frac{1}{d^2} \sum_{i,j=1}^{d} Tr\left(E_i^{(U)} \otimes E_j^{(U)} F_{ij}^{(U)} \right)$$

Realizácia optimálneho 2→1 klonovania POVM



$$P_1 = \frac{(9d(d+1)-2)}{9d(d+1)}|+\rangle\langle+|$$

$$P_2 = |\psi\rangle\langle\psi| \quad P_3 = \sigma_z|\psi\rangle\langle\psi|\sigma_z$$

$$|\psi\rangle = \sqrt{\frac{1}{9d(d+1)}}\,|+\rangle + \sqrt{\frac{1}{2}}\,|-\rangle$$

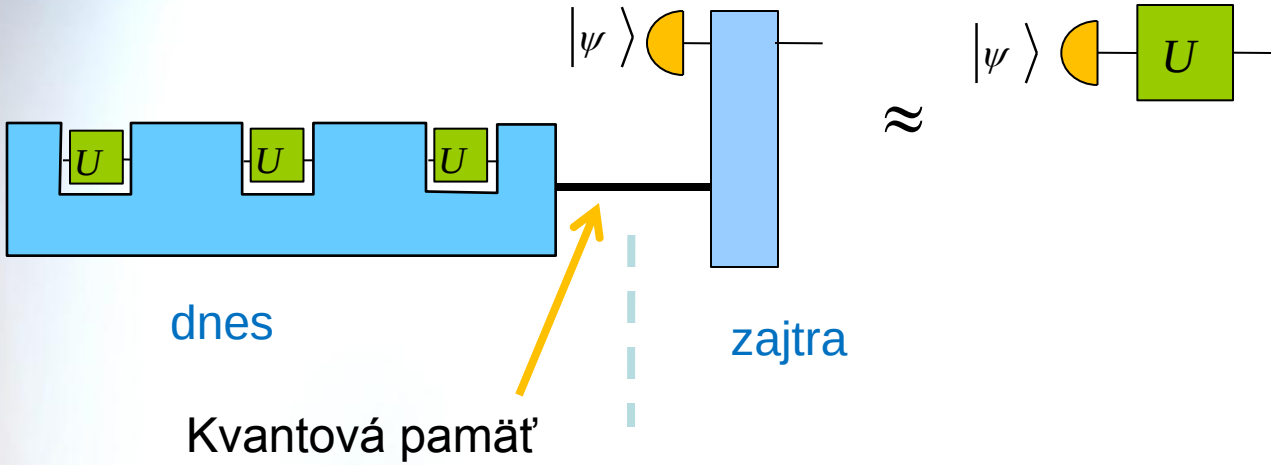
$$f(k,n) = \begin{cases} (k,k) & \text{if } n=1 \\ (k,j) \quad j\neq k & \text{if } n=2 \\ (j,k) \quad j\neq k & \text{if } n=3 \end{cases}$$

- Realizácia vyžaduje iba jeden pomocný qubit
- Qubit treba zmerať 3-výsledkovým POVM

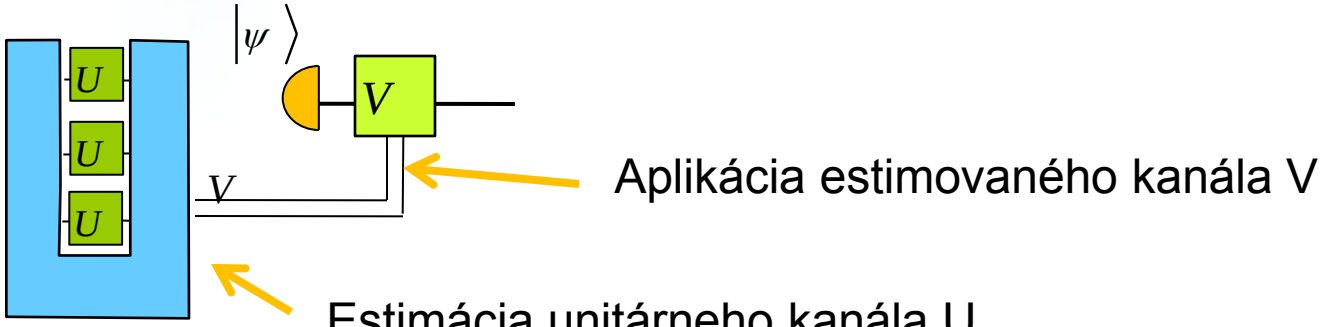
A. Bisio, G. M. D'Ariano, P. Perinotti, M. Sedlák, Phys. Rev. A 84, 042330 (2011)

Learning unitárneho kanála

Cost funkcia je opäť Channel Fidelity



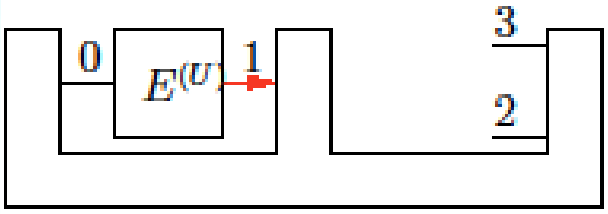
Optimálna stratégia:



A. Bisio, G. Chiribella, G. M. D'Ariano, S. Facchini, P. Perinotti, Phys. Rev. A 81, 032324 (2010)

1→2 **Learning** vs. **Cloning** POVM

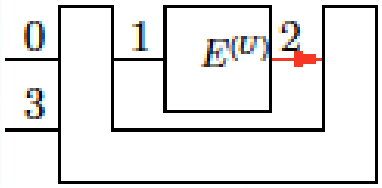
Learning:



$$F = \frac{9d^2 + 16d - 17}{6d^2\left(d^2 - 1\right)} \square \frac{3}{2d^2}$$

Cloning:

Stratégie pre klonovanie zahŕňajú learning stratégie

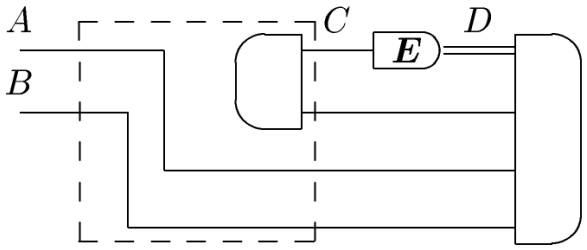


$$F = \frac{4}{3d}$$

$$F_{clon} \geq F_{learn}$$

pretože:

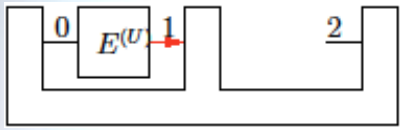
- Podobne ako pre cloning vs. learning unitárnych kanálov klonovanie je o jeden rád lepšie



Výsledky optimalizácie

N→1 Learning quditového POVM

1→1 Learning:



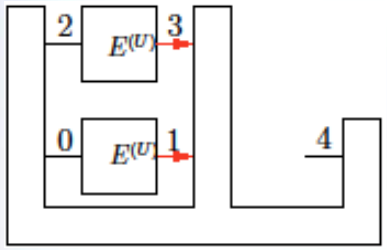
pre qubity:

$$F = 0,75$$

pre qudity:

$$F = \frac{d+1}{d^2}$$

2→1 Learning:

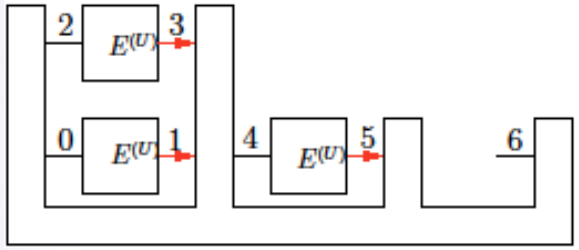


$$F = 0,811$$

$$F = \frac{d(d+1)^2 - 2 + \sqrt{d^4 - 2d^2 + 5}}{d(d-1)(d+1)^2}$$

Optimálna stratégia je **paralelná**

3→1 Learning:



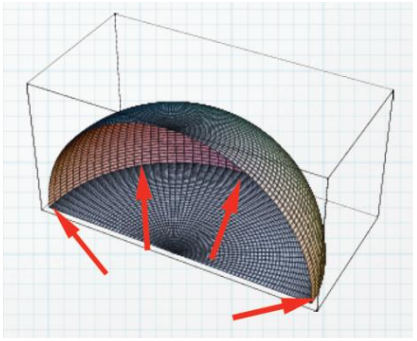
$$F = 0,868$$

Optimálna stratégia je **sekvenčná**

A. Bisio, G. M. D'Ariano, P. Perinotti, M. Sedlák, Physics Letters A 375, pp. 3425 (2011)

Extremálnosť kvantových hrebeňov

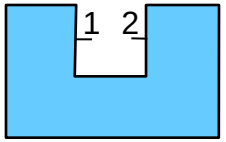
- Množina kvantových hrebeňov a ich inštrumentov (quantum comb instruments) je **konvexná**



- **Extremálne body** charakterizujú množinu a sú riešeniami optimalizácie pre konkávné cost-funkcie

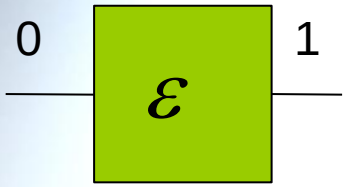
Výsledky publikovaného článku:

- N&S podmienka extremality pre všeobecný inštrument (zahŕňa kanály, inštrumenty)
- Nerovnosť pre ranky elementov 1-testera
- Klasifikácia 1-testerov
- príklady qubitových 1-testerov



G. M. D'Ariano, P. Perinotti, M. Sedlák, J. Math. Phys. 52, 082202 (2011)

Extremálnosť kvantových kanálov



Kanál = GQI s jediným výsledkom a jedným vstupom, výstupom

Double Ket notácia: $\left|A\right\rangle\!\right\rangle \equiv A \otimes I \sum_i \left|i\right\rangle\left|i\right\rangle$

$$E = \varepsilon \otimes \mathbf{1}\left(\left|I\right\rangle\!\right\rangle\left\langle\!\left\langle I\right|\right) = \sum_{n=1}^{r} \left|K_n\right\rangle\!\right\rangle\left\langle\!\left\langle K_n\right|$$

K_i minimálna Krausová reprezentácia pre $\mathcal{E}$

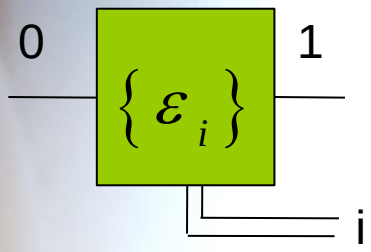
$$W \equiv \left\{\sigma_k \otimes \mathbf{1}_0, \forall k\right\} \bigcup \left\{\sigma_k \otimes \sigma_l, k \neq l\right\}$$

$$\sum_i \sum_{n,m} D_{nm} \left|K_n\right\rangle\!\right\rangle\left\langle\!\left\langle K_m\right| + \sum_k \alpha_k \sigma_k \otimes \mathbf{1}_2 + \sum_{k,l} \beta_{kl} \sigma_k \otimes \sigma_l = 0$$

Podmieku môžeme ekvivalentne prepísať ako Choi-ovú podmienku lineárnej nezávislosti pre:

$$\left(K_n\right)^+ K_m \qquad \forall n, m$$

Extremalita inštrumentov



Inštrument

- Popisuje kvantové meranie s klasickým aj kvantovým výstupom
- GQI s **M výsledkami** a jedným vstupným, výstupným priestorom

$$\mathcal{E}_i(\rho) = \sum_n K_n^i \rho K_n^{i+}$$

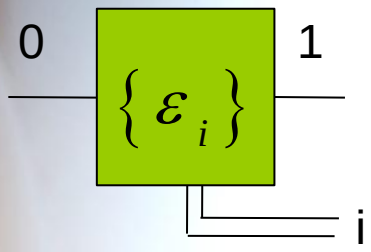
$$W \equiv \{\sigma_k \otimes \mathbf{1}_0, \forall k\} \cup \{\sigma_k \otimes \sigma_l, k \neq l\}$$

$$\sum_i \sum_{n,m} D_{nm}^i \left|K_n^i\right\rangle\!\left\rangle\!\left\langle\!\left\langle K_m^i\right|\right. + \sum_k \alpha_k \sigma_k \otimes \mathbf{1}_2 + \sum_{k,l} \beta_{kl} \sigma_k \otimes \sigma_l = 0$$

Podmieku môžeme ekvivalentne prepísať ako podmienku lineárnej nezávislosti pre:

$$\left(K_n^i\right)^+ K_m^i \qquad \forall i, n, m$$

POVM and kanál indukovaný inštrumentom



Ignorovaním kvantového výstupu inštrumentu získame POVM

$$P_i = \sum_n \left(K_n^i\right)^+ K_n^i$$

Ignorovaním klasického výstupu inštrumentu získame kanál

$$\mathcal{E}(\rho) = \sum_i \mathcal{E}_i(\rho) = \sum_i \sum_n K_n^i \rho K_n^{i+}$$

Lüdersov inštrument =

Inštrument definovaný POVM $\{P_i\}_{i=1}^M$ ako $\mathcal{E}_i(\rho) = \sqrt{P_i}\,\rho\,\sqrt{P_i}$

Lüdersové inštrumenty sú extremálne práve vtedy keď, sú elementy POVM lineárne nezávislé

Zhrnutie

Kvantové hrebene sú veľmi užitočné pre:

- Optimalizácia kvantových algoritmov
- analýza pamäťových efektov a nárokov
- Riešenie problémov s obmedzenými zdrojmi
- Analýza komunikačných protokolov

O čom som nehovoril:

- Dôkaz nerealizovateľnosti Quantum bit commitmentu
- Operačná vzdialenosť pre kvantové hrebene
- aplikácia hrebeňov pre všeobecné pravdepodobnostné teórie
- kompresia pamäte protokolov
- Všeobecné transformácie unitárnych kanálov

References:

Články o kvantových hrebeňoch na ktorých som sa podielal:

D'Ariano, Perinotti, MS, “Extremal quantum protocols", J. Math. Phys. 52, 082202 (2011)

Bisio, D'Ariano, Perinotti, MS, „Quantum learning ...“, Phys. Lett. A 375, pp. 3425 (2011)

Bisio, D'Ariano, Perinotti, MS, „Cloning of measurement “, Phys.Rev.A 84,042330 (2011)

Q. Comb framework:

G. Chiribella, G. M. D'Ariano, P. Perinotti, “Theoretical framework for quantum networks”, Phys. Rev. A 80, 022339 (2009),

G. Chiribella, G. M. D'Ariano, P. Perinotti, “Quantum circuits architecture”, Phys. Rev. Lett. 101, 060401 (2008),

Ďalšie aplikácie kvantových hrebeňov:

(authors: A. Bisio, G. Chiribella, G. M. D'Ariano, S. Facchini, P. Perinotti)

“Information - Disturbance Tradeoff in Estimating a Unitary Transformation”, arXiv:1006.5665

“Minimal computational-space implementation of multi-round quantum protocols”, arXiv:1006.1780

“Optimal quantum learning of a unitary transformation”, Phys. Rev. A 81, 032324 (2010)

“Optimal quantum tomography for states, measurements, and transformations”, Phys. Rev. Lett. 102 (2009) 010404

Ďakujem za pozornosť.