7^{th} Workshop in Quantun Information Processing, Waterloo, Canada, January 16^{th}, 2004

Quantum symmetric group problems

Julia Kempe

UC Berkeley and LRI, Orsay, France

joint works with

Aner Shalev (Hebrew University) and

Joshua von Korff (UC Berkeley)

Outline

Two Results:

1. The hidden subgroup problem and permutation groups (with A. Shalev) – a characterisation of distinguishable subgroups
2. The lost permutation problem (with J. von Korff) – a quantum over classical improvement in transmitting permutations through a shuffling channel

Some proofs and explanations

Quantum Fourier Sampling and the Hidden Subgroup Problem over the symmetric group

Hidden subgroups of S_n

Quantum Fourier Sampling (QFS) can solve the Hidden Subgroup Problem (HSP) for **Abelian** groups (Shor's algorithm, discrete log)

HSP: $H < G$ $\qquad f : G \to R$

$\forall h \in H$ $\qquad f(x) = f(xh)$

Promise: f is constant on cosets of H and distinct on different cosets.

Task: find a set of generators for H.

Hidden subgroups of S_n

Quantum Fourier Sampling (QFS) can solve the Hidden Subgroup Problem (HSP) for **Abelian** groups (Shor's algorithm, discrete log)

What about non-Abelian groups?

Symmetric group – would imply solution to the graph isomorphism/automorphism problem.

(Abelian groups have one-dimensional irreducible representations.)

Hidden subgroups of S_n

Only few known results on non-Abelian groups:

Efficient solutions for:

- *Dihedral group* – information theoretic solution to HSP [Ettinger,Hoyer'99], exponential classical postprocessing (or subexp algorithm [Kuperberg03])

  (dihedral group: irreps have small dimension)

Hidden subgroups of S_n

Only few known results on non-Abelian groups:

Efficient solutions for:

- *Dihedral group* – information theoretic solution to HSP [Ettinger,Hoyer'99], exponential classical postprocessing (improved to subexp [Kuperberg03])

  (dihedral group: irreps have small dimension)
- *Normal subgroups* ($gHg^{-1}=H$) [Hallgren et al.'00]
- *Some semidirect products* and *wreath products* of Abelian groups [Roetteler,Beth'98], [Grigni et al.'01], affine groups [Moore et al.'04]
- Groups with *small commutator groups* [Ivanyos et al.'01], *solvable groups of constant exponent*

  [Friedl et al.'03]…

Hidden subgroups of S_n

All this does not apply to the symmetric group S_n!

- Subgroups are *far from normal*

  (lots of conjugate subgroups gHg^{-1})
- Most Irreps are *large* ($2^{\theta(n \log n)}$)
- Only *partial explicit knowledge* about irreps and characters

Crash-course in representation theory

Representation: $\rho : G \to GL(d)$ GL(d) = d-by-d matrices

preserves group structure of G (*homomorphism*)

$$\rho(g_1 \circ g_2) = \rho(g_1)\rho(g_2)$$

Irreducible representation (irrep): does not split into a (common) block structure in some basis

Crash-course in representation theory

Representation: $\rho : G \to GL(d)$ GL(d) = d-by-d matrices

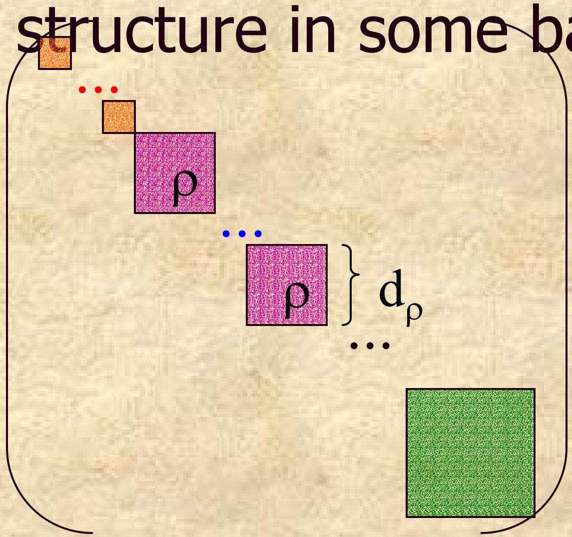
preserves group structure of G (*homomorphism*)

$$\rho(g_1 \circ g_2) = \rho(g_1)\rho(g_2)$$

dim $\rho = d_\rho$

***Irreducible* representation (irrep):** does not split into a (common) block structure in some basis

$\rho(g) \neq$



Every representation splits into irreps.

Character:

$$\chi(g) = tr\,\rho(g)$$

$$\chi(g) = \chi(hgh^{-1})$$

Crash-course in representation theory

Orthogonality relations:

the vectors $\frac{1}{\sqrt{|G|}} \sum_{\rho,i,j} \sqrt{d_\rho}\, \rho(g)_{ij} \, |\rho,i,j\rangle$ are orthonormal

---

Representation: $\rho : G \to GL(d)$ GL(d) = d-by-d matrices

preserves group structure of G (*homomorphism*)

$$\rho(g_1 \circ g_2) = \rho(g_1)\rho(g_2)$$

dim $\rho = d_\rho$

Quantum Fourier Sampling

Quantum Fourier Sampling (QFS) can solve the Hidden Subgroup Problem (HSP) for Abelian groups

(Shor's algorithm, discrete log)

QFS:

1) uniform superposition over G

$$|s\rangle|0\rangle = \frac{1}{|G|}\sum_{g\in G}|g\rangle|0\rangle$$

QFS

QFS:

1) uniform superposition over G $\qquad |s\rangle|0\rangle = \frac{1}{|G|}\sum_{g\in G}|g\rangle|0\rangle$

2) Apply f, measure (or trace) second register

$$\sum_{g\in G}|g\rangle|f(g)\rangle \rightarrow |gH\rangle = \frac{1}{\sqrt{|H|}}\sum_{h\in H}|gh\rangle$$

QFS

QFS:

1) uniform superposition over G $$|s\rangle|0\rangle = \frac{1}{|G|}\sum_{g\in G}|g\rangle|0\rangle$$

2) Apply f, measure (or trace) second register

$$\sum_{g\in G}|g\rangle|f(g)\rangle \rightarrow |gH\rangle = \frac{1}{\sqrt{|H|}}\sum_{h\in H}|gh\rangle$$

3) QFT

$$|g\rangle \rightarrow \frac{1}{\sqrt{|G|}}\sum_{\rho,\mathrm{i,j}}\sqrt{d_\rho}\,\rho(g)_{\mathrm{ij}}\,|\rho,\mathrm{i,j}\rangle$$

QFS

QFS:

1) uniform superposition over G

$$|s\rangle|0\rangle = \frac{1}{|G|}\sum_{g\in G}|g\rangle|0\rangle$$

2) Apply f, measure (or trace) second register

$$\sum_{g\in G}|g\rangle|f(g)\rangle \rightarrow |gH\rangle = \frac{1}{\sqrt{|H|}}\sum_{h\in H}|gh\rangle$$

3) QFT

$$|g\rangle \rightarrow \frac{1}{\sqrt{|G|}}\sum_{\rho,i,j}\sqrt{d_\rho}\,\rho(g)_{ij}|\rho,i,j\rangle$$

Note: for Abelian groups d_ρ=1 and $\rho(g)=\chi(g)$

$$|g\rangle \rightarrow \frac{1}{\sqrt{|G|}}\sum_{\chi}\chi(g)|\chi\rangle$$

QFS

QFS:

1) uniform superposition over G $$|s\rangle|0\rangle = \frac{1}{|G|}\sum_{g\in G}|g\rangle|0\rangle$$

2) Apply f, measure (or trace) second register

$$\sum_{g\in G}|g\rangle|f(g)\rangle \rightarrow |gH\rangle = \frac{1}{\sqrt{|H|}}\sum_{h\in H}|gh\rangle$$

3) QFT

$$|g\rangle \rightarrow \frac{1}{\sqrt{|G|}}\sum_{\rho,\mathrm{i,j}}\sqrt{d_\rho}\,\rho(g)_{\mathrm{ij}}|\rho,\mathrm{i,j}\rangle$$

gives $$\frac{1}{\sqrt{|G||H|}}\sum_{\rho,\mathrm{i,j}}\sqrt{d_\rho}\sum_{h\in H}\rho(gh)_{\mathrm{ij}}|\rho,\mathrm{i,j}\rangle$$ with random g

QFS

QFS:

1) uniform superposition over G $\quad |s\rangle|0\rangle = \frac{1}{|G|}\sum_{g\in G}|g\rangle|0\rangle$

2) Apply f, measure (or trace) second register

$$\sum_{g\in G}|g\rangle|f(g)\rangle \rightarrow |gH\rangle = \frac{1}{\sqrt{|H|}}\sum_{h\in H}|gh\rangle$$

3) QFT

$$|g\rangle \rightarrow \frac{1}{\sqrt{|G|}}\sum_{\rho,\mathrm{i,j}}\sqrt{d_\rho}\,\rho(g)_{\mathrm{ij}}|\rho,\mathrm{i,j}\rangle$$

gives $\quad \frac{1}{\sqrt{|G||H|}}\sum_{\rho,\mathrm{i,j}}\sqrt{d_\rho}\sum_{h\in H}\rho(gh)_{\mathrm{ij}}|\rho,\mathrm{i,j}\rangle \quad$ with random g

4) Sample (measure): probability distribution

$$P_{gH}(\rho,i,j) = \frac{d_\rho}{|G||H|}\left|\sum_{h\in H}\rho(gh)_{ij}\right|^2$$

QFS

Probability distribution:

Weak form: sample ρ only (average over i,j)

$$P_{gH}(\rho) = \sum_{i,j} P_{gH}(\rho, i, j) = \frac{d_\rho}{|G||H|} \sum_{i,j} \left| \sum_{h \in H} \rho(gh)_{ij} \right|^2 = \frac{d_\rho}{|G|} \sum_{h \in H} \chi(h) = P_H(\rho)$$

Remark: Same distribution for all conjugate subgroups $H' = gHg^{-1}$ (cyclic property of trace).

QFS

Probability distribution:

Weak form: sample ρ only (average over i,j)

$$P_{gH}(\rho)=\sum_{i,j}P_{gH}(\rho,i,j)=\frac{d_\rho}{|G||H|}\sum_{i,j}\left|\sum_{h\in H}\rho(gh)_{ij}\right|^2=\frac{d_\rho}{|G|}\sum_{h\in H}\chi(h)=P_H(\rho)$$

Remark: Same distribution for all conjugate subgroups

$H'=gHg^{-1}$ (cyclic property of trace).

Strong form: sample ρ, i, j in some basis

Choice of basis is arbitrary…

Hidden subgroups of S_n

Previous results for QFS of S_n (Hallgren,Russel,TaShma'00, Grigni,Schulman, Vazirani, Vazirani '01) :

- Strong form: *rows* provide no additional information (the distribution on rows is always uniform) [GSVV'01]

Hidden subgroups of S_n

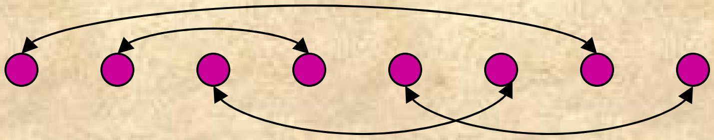
Previous results for QFS of S_n (Hallgren et al.'00, Grigni et al. '01) :

- Strong form: *rows* provide no additional information (the distribution on rows is always uniform for all G) [GSVV'01]
- Strong form with (uniformly) random basis: *columns* provide exponentially small extra information for S_n [GSVV'01]

Hidden subgroups of S_n

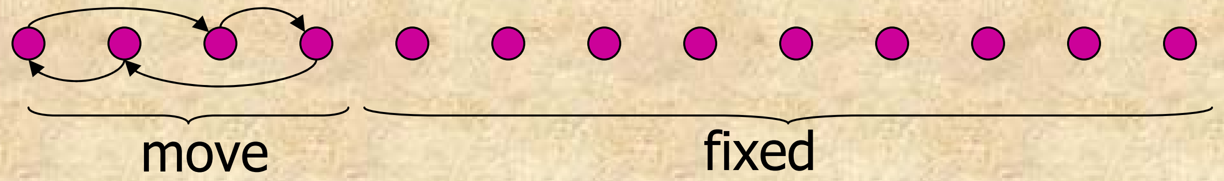
Previous results for QFS of S_n (Hallgren et al.'00, Grigni et al. '01) :

- Strong form: *rows* provide no additional information (the distribution on rows is always uniform) [GSVV'01]
- Strong form with (uniformly) random basis: *columns* provide exponentially small extra information [GSVV'01]
- Weak form: cannot distinguish involution with n/2 2-cycles from {e} in time poly(n).



Hidden subgroups of S_n

Definition: permutation of constant support = permutation in which all but a constant number of points are fixed

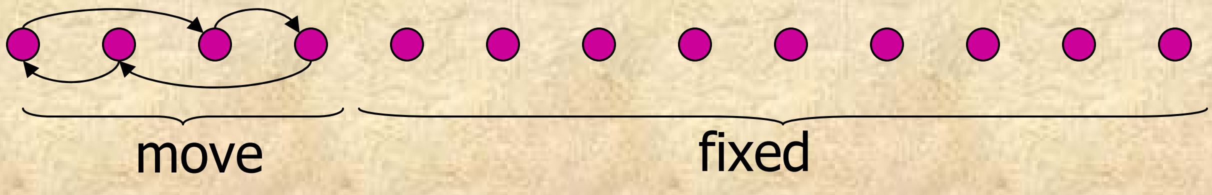


Hidden subgroups of S_n

Results for S_n (joint with Aner Shalev) :

♠ H can be distinguished from {e} * only if it contains an element of constant support.

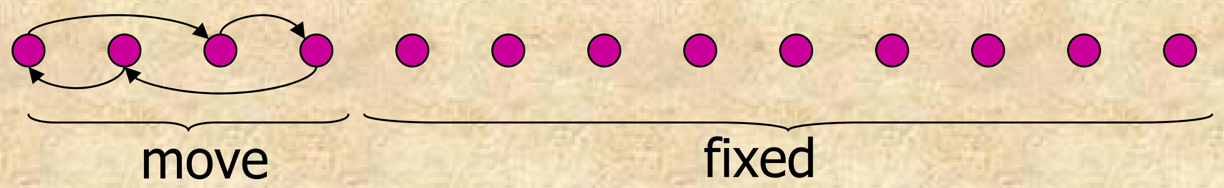
- If H is of polynomial size (in n) (♠ : iff)
- If H is primitive (building blocks of all $H \subseteq S_n$)
- For a family of subgroups of superexponential order
- Given a group theoretic conjecture, ♠ is true for all H



*with either the weak standard method or the strong standard method with random basis

Hidden subgroups of S_n

Definition: permutation of constant support = permutation in which all but a constant number of points are fixed



Remark: There are only poly(n) permutations of constant support. They can be enumerated (checked) in polynomial time.

Hidden subgroups of S_n

Results for S_n (joint with Aner Shalev) :

♠ H can be distinguished from {e} * only if it contains an element of constant support.

- If H is of polynomial size (in n) (♠: iff)
- If H is primitive (building blocks of all H
- For a family of subgroups of superexponential order
- Given a group theoretic conjecture, ♠ is true for all H

Quantum Fourier Sampling* has no advantage over classical exhaustive search (check all elements of constant support)!

*with either the weak standard method or the strong standard method with random basis

Hidden subgroups of S_n

Probability distribution from QFS:

Weak form:

$$P_{gH}(\rho)=\sum_{i,j}P_{gH}(\rho,i,j)=\frac{d_\rho}{|G||H|}\sum_{i,j}\left|\sum_{h\in H}\rho(gh)_{ij}\right|^2=\frac{d_\rho}{|G|}\sum_{h\in H}\chi(h)=P_H(\rho)$$

Total distribution distance between P_H and $P_{\{e\}}$:

$$D_H=\frac{1}{|G|}\sum_\rho d_\rho\left|\sum_{h\in H,h\neq e}\chi_\rho(h)\right|$$

Hidden subgroups of S_n

Probability distribution from QFS:

Weak form:

$$P_{gH}(\rho)=\sum_{i,j}P_{gH}(\rho,i,j)=\frac{d_\rho}{|G||H|}\sum_{i,j}\left|\sum_{h\in H}\rho(gh)_{ij}\right|^2=\frac{d_\rho}{|G|}\sum_{h\in H}\chi(h)=P_H(\rho)$$

Total distribution distance between P_H and $P_{\{e\}}$:

$$D_H=\frac{1}{|G|}\sum_{\rho}d_\rho\left|\sum_{h\in H,h\neq e}\chi_\rho(h)\right|$$

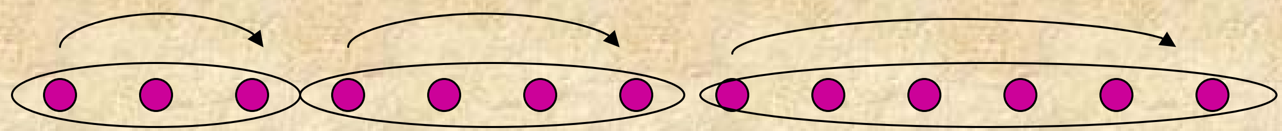
H and {e} efficiently distinguishable information-theoretically iff $D_H\geq\left(\log|G|\right)^{-c}=\mathrm{n}^{-c'}$

Hidden subgroups of S_n

Definition: Conjugacy class C– set closed under conjugation by elements in G

$$C_h = \{ghg^{-1} : \forall g \in G\}$$

For S_n: Conjugacy class of π= permutations with the same cycle structure



Hidden subgroups of S_n

$$D_H = \frac{1}{|G|}\sum_{\rho} d_\rho \left| \sum_{h\in H, h\neq e} \chi_\rho(h) \right|$$

Main tool:

Lemma: $C_1,\ldots,C_k$ – non-identity conjugacy classes of G.

$$\sum_{i=1}^{k} |C_i \cap H|^2 |H|^{-1} |C_i|^{-1} < D_H < \sum_{i=1}^{k} |C_i \cap H| |C_i|^{-1/2}$$

Hidden subgroups of S_n

$$D_H = \frac{1}{|G|}\sum_{\rho} d_\rho \left| \sum_{h\in H, h\neq e} \chi_\rho(h) \right|$$

Main tool:

Lemma: $C_1,\ldots,C_k$ – non-identity conjugacy classes of G.

$$\sum_{i=1}^{k} |C_i \cap H|^2 |H|^{-1} |C_i|^{-1} < D_H < \sum_{i=1}^{k} |C_i \cap H| |C_i|^{-1/2}$$

Corollary 1: C_{min} of minimal size intersecting H

$$|H|^{-1} |C_{min}|^{-1} < D_H < (|H|-1) |C_{min}|^{-1/2}$$

Hidden subgroups of S_n

Main tool:

Corollary 1: C_{min} of minimal size intersecting H

$$|H|^{-1}|C_{min}|^{-1} < D_H < (|H|-1)|C_{min}|^{-1/2}$$

Remark: $g \in S_n$ has support k. Then $\left(\frac{n}{e}\right)^k \leq \binom{n}{k} \leq C_g \leq n^k$

$n^{-c'} < (|H|-1)|C_{min}|^{-1/2} < D_H$ and $|H|=poly(n)=n^c$

$\Rightarrow$ distinguishable iff k=const.

Hidden subgroups of S_n

Main tool:

Corollary 1: C_{min} of minimal size intersecting H

$$|H|^{-1}|C_{min}|^{-1} < D_H < (|H|-1)|C_{min}|^{-1/2}$$

Remark: $g \in S_n$ has support k. Then $\left(\frac{n}{e}\right)^k \leq \binom{n}{k} \leq C_g \leq n^k$

$$n^{-c'} < (|H|-1)|C_{min}|^{-1/2} < D_H$$ and $|H| = poly(n) = n^c$

$\Rightarrow$ distinguishable iff k=const.

Corollary 2: If |H|=poly(n): distinguishable iff H contains an element of constant support.

Main tool

$$D_H = \frac{1}{|G|}\sum_{\rho} d_\rho \left| \sum_{h\in H, h\neq e} \chi_\rho(h) \right|$$

Lemma: $C_1,\ldots,C_k$ – non-identity conjugacy classes

$$\sum_{i=1}^{k} |C_i \cap H|^2 |H|^{-1} |C_i|^{-1} < D_H < \sum_{i=1}^{k} |C_i \cap H| |C_i|^{-1/2}$$

Proof idea of upper bound:

$$\sum_{\rho} d_\rho \left| \sum_{h\in H, h\neq e} \chi_\rho(h) \right| \leq \sum_{\rho} d_\rho \sum_{h\in H, h\neq e} |\chi_\rho(h)|$$

$$\sum_{\rho} d_\rho |\chi_\rho(h)| \leq \sqrt{\sum_{\rho} d_\rho^{\,2}} \sqrt{\sum_{\rho} |\chi_\rho(h)|^2} \leq \sqrt{|G|} \sqrt{|G| / |C_h|} = |G| |C_h|^{-1/2}$$

Main tool

$$D_H = \frac{1}{|G|}\sum_\rho d_\rho \left|\sum_{h\in H, h\neq e} \chi_\rho(h)\right|$$

Lemma: $C_1,\ldots,C_k$ – non-identity conjugacy classes

$$\sum_{i=1}^{k} |C_i \cap H|^2 |H|^{-1} |C_i|^{-1} < D_H < \sum_{i=1}^{k} |C_i \cap H| |C_i|^{-1/2}$$

Proof idea of lower bound:

$$\left|\sum_{h\in H, h\neq e} \chi_\rho(h)\right| \leq \sum_{h\in H, h\neq e} |\chi_\rho(h)| \leq \sum_{h\in H, h\neq e} d_\rho \leq |H| d_\rho$$

$$d_\rho > |H|^{-1} \left|\sum_{h\in H, h\neq e} \chi_\rho(h)\right|$$

$$\chi_\rho(h) = \chi_\rho(C_i) \quad \text{if} \quad h \in H \cap C_i$$

$$D_H > \frac{1}{|G||H|}\sum_\rho \left|\sum_{h\in H, h\neq e} \chi_\rho(h)\right|^2 = \frac{1}{|G||H|}\sum_\rho \left|\sum_{i=1}^{k} |H\cap C_i| \chi_\rho(C_i)\right|^2$$

Generalized orthogonality relations …

Hidden subgroups of S_n

Theorem: $H<S_n$ of non-constant support. If for all $k \leq n$ H has at most $n^{k/7}$ elements of support $\leq k$ then H indistinguishable.

Hidden subgroups of S_n

Theorem: $H<S_n$ of non-constant support. If for all $k \le n$ H has at most $n^{k/7}$ elements of support $\le k$ then H indistinguishable.

Group theoretic conjecture: $H<S_n$ of non-constant support. For all $k \le n$ H has at most $n^{k/7}$ elements of support $\le k$ (true for *primitive groups, family of superexponentially large groups*).

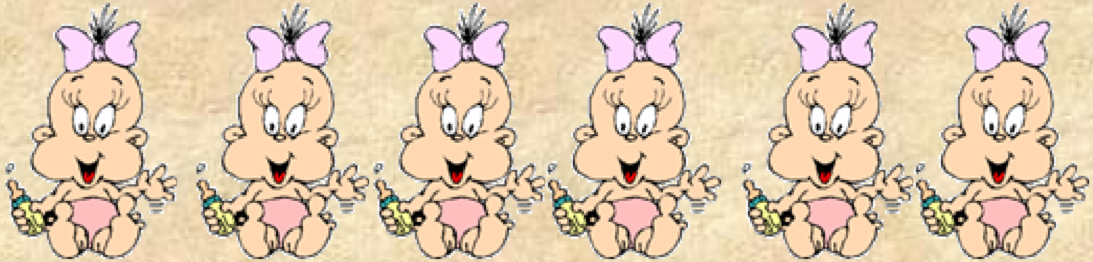
Implies: If H distinguishable $\Rightarrow$ H has constant minimal support (♠).

➡ QFS is no stronger than classical exhaustive search (only poly many elements of constant degree).

Permutation transmission through a shuffling channel
or
the prolific family problem

The prolific-family problem

Hexa-plets:



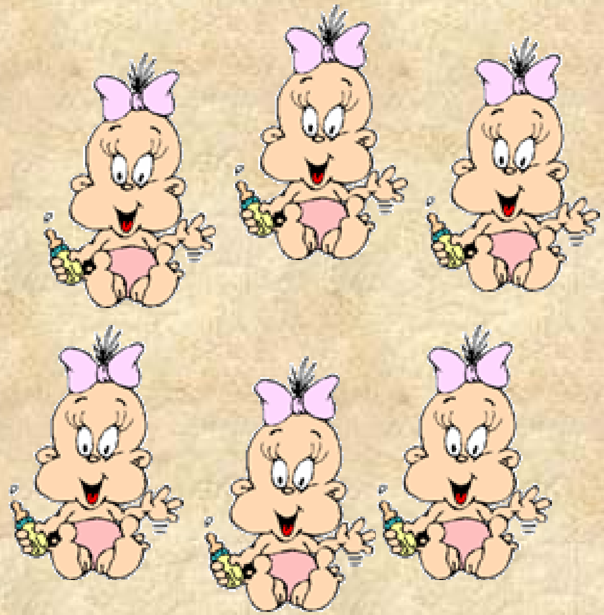
Alice Babe Chiquita Dina Emily Faye …

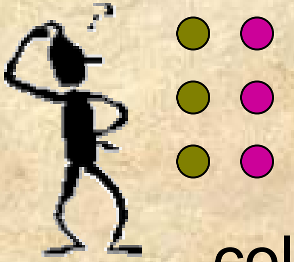
The prolific- family problem

Hexa-plets:

The prolific- family problem

Hexa-plets:



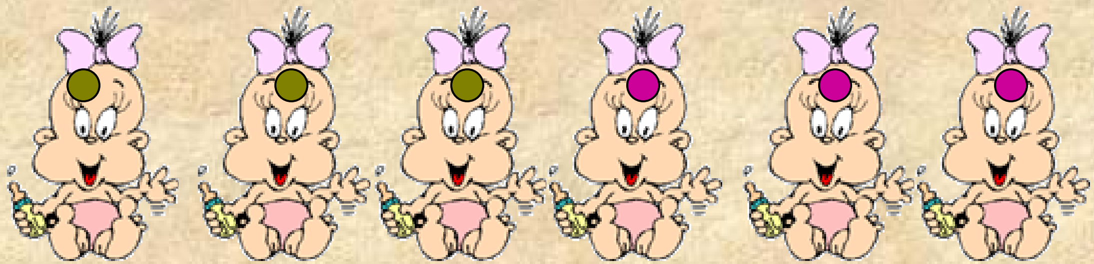


color !!!

Alice Babe Chiquita Dina Emily Faye

The prolific- family problem

Hexa-plets:



Alice Babe Chiquita Dina Emily Faye …

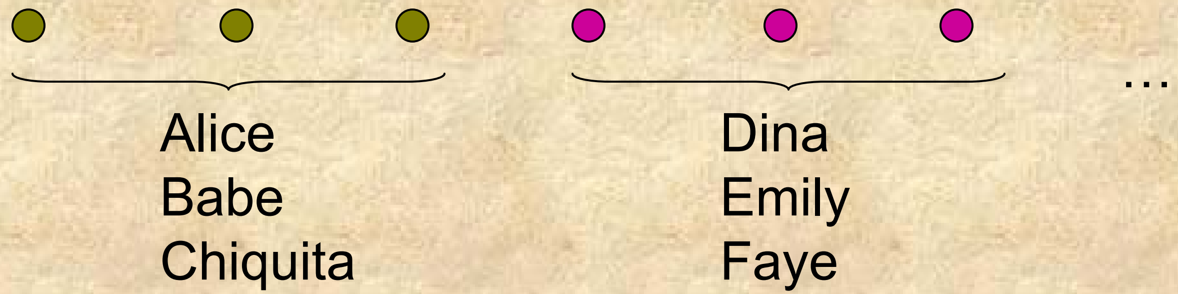
2 colors, n babies:

Task: restore the original order exactly after random shuffling

- best strategy: n/2 green, n/2 red

The prolific- family problem

Hexa-plets:



2 colors, n babies:

Task: restore the original order exactly after random shuffling

- best strategy: n/2 in green, n/2 red
- success probability:

$$p_c = \frac{1}{\left(\frac{n}{2}!\right)^2}$$

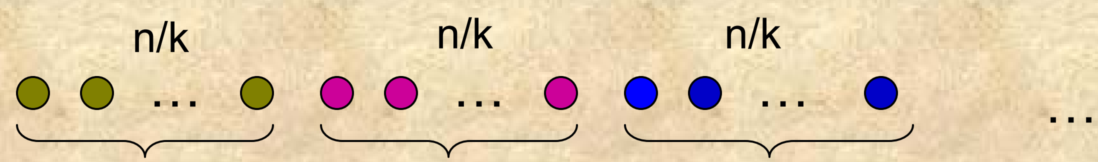
The p-f problem

General problem: encode a permutation optimally aga shuffling noise

k colors (log k bits per item), n items:

- best strategy: k blocks of size n/k in one color
- success probability:

$$p_c(k) = \frac{1}{\left(\frac{n}{k}!\right)^k}$$



$$p = \frac{1}{\left(\frac{n}{k}!\right)} \qquad p = \frac{1}{\left(\frac{n}{k}!\right)} \qquad p = \frac{1}{\left(\frac{n}{k}!\right)}$$

Need k=n colors to obtain success probability p=1!

The p-f problem

Qubits instead of bits?

k quantum “colors” states (log k qubits per item), n items:

$|●\rangle + |●\rangle + |●\rangle + \ldots$

$$p_c(k) = \frac{1}{\left(n/k\,!\right)^k}$$

The p-f problem

Qubits instead of bits?

k quantum “colors” states (log k qubits per item), n items:

|●⟩ + |●⟩ + |●⟩ +…

$$p_c(k) = \frac{1}{\left(\frac{n}{k}!\right)^k}$$

Results (joint with Joshua von Korff):

- quantum success probability:

$$p_q(k) = \frac{k^n - o(k^n)}{n!}$$

(for $k < \frac{1}{5}\sqrt{n}$)

The p-f problem

Qubits instead of bits?

k quantum "colors" states (log k qubits per item), n items:

$|\bullet\rangle + |\bullet\rangle + |\bullet\rangle + \dots$

Results (joint with Joshua von Korff):

$$p_c(k) = \frac{1}{\left(n/k!\right)^k}$$

- quantum success probability:

$$p_q(k) = \frac{k^n - o(k^n)}{n!} \quad \text{for} \quad k < \frac{1}{5}\sqrt{n}$$

$$\frac{p_q(k)}{p_c(k)} \to \frac{(2\pi n)^{(k-1)/2}}{k^{k/2}}$$

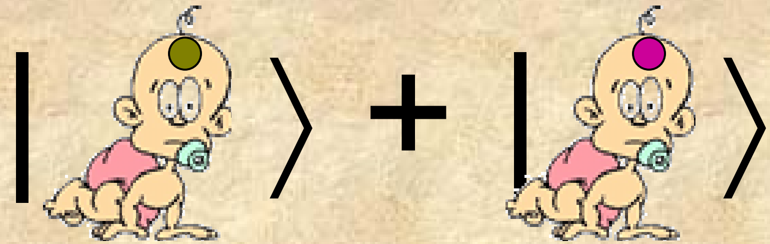
Conjecture: true for all k (probably true)

⇨Need $k \approx n/e$ colors to obtain success probability p=1!
(k=n classically)

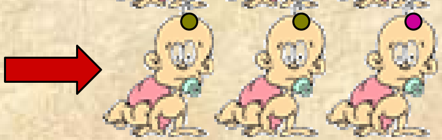
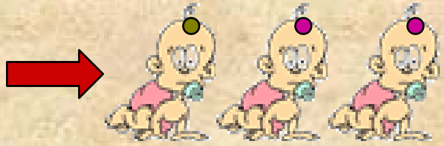
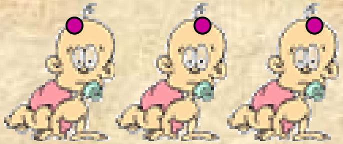
The p-f problem

Example: triplets

2 quantum states :



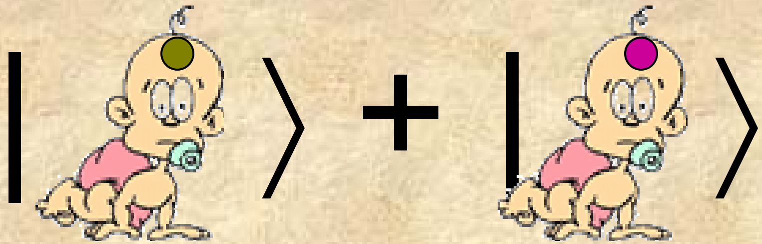
Classical Options:

A B C	p
	1/6
	½
	½
	1/6

The p-f problem

Example: triplets

2 quantum states :

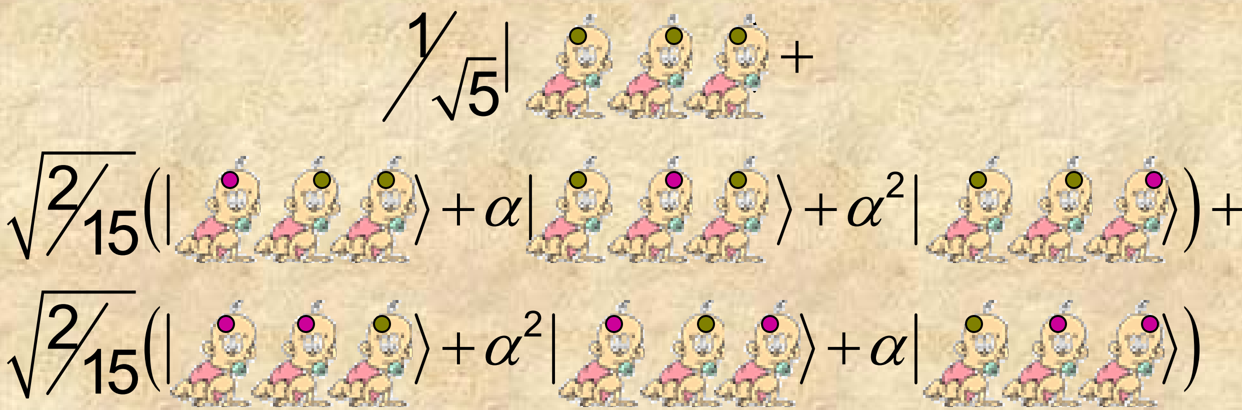


Classical Options:

A B C p

½

Quantum solution: $(\alpha^3 = 1)$

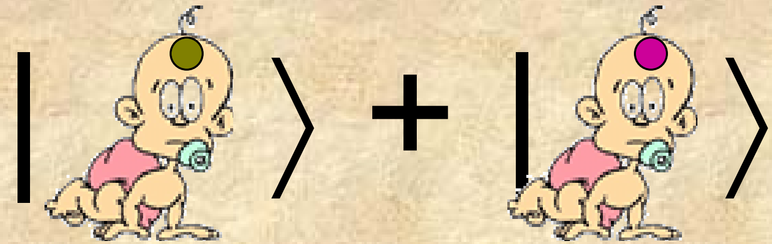


Quantum success probability: p=5/6

The p-f problem

Example: triplets

2 quantum states :

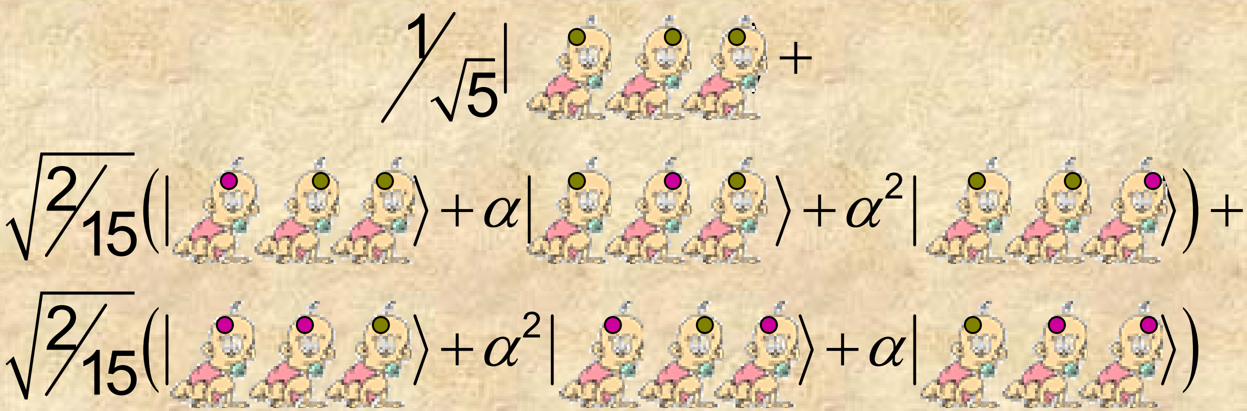


Classical Options:

A B C p

½

Quantum solution: $(\alpha^3 = 1)$



Quantum success probability: p=5/6

$$p_{quantum} = \frac{2^n - n}{n!}$$

$$p_{classical} = \frac{1}{(n/2!)^2}$$

$$\frac{p_{quantum}}{p_{classical}} \to \sqrt{n}$$

The p-f problem $|$  $\rangle + |$  $\rangle$

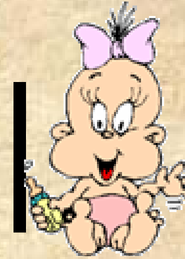
Quantum solution: $(\alpha^3 = 1)$

$$|\psi\rangle = \frac{1}{\sqrt{5}}|000\rangle + \sqrt{\frac{2}{15}}\left(|100\rangle + \alpha|010\rangle + \alpha^2|001\rangle\right) + \sqrt{\frac{2}{15}}\left(|110\rangle + \alpha^2|101\rangle + \alpha|011\rangle\right)$$

$|\psi\rangle$ chosen such that set of permutations of $|\psi\rangle$
"as orthogonal as possible"

$$S_3 = \{s_i : i = 1..6\} = \{id,(12),(13),(23),(231),(312)\}$$

The p-f problem

$|$  $\rangle$ + $|$  $\rangle$

Quantum solution: $(\alpha^3 = 1)$

$$|\psi\rangle = \tfrac{1}{\sqrt{5}}|000\rangle + \sqrt{\tfrac{2}{15}}\left(|100\rangle + \alpha|010\rangle + \alpha^2|001\rangle\right) + \sqrt{\tfrac{2}{15}}\left(|110\rangle + \alpha^2|101\rangle + \alpha|011\rangle\right)$$

$|\psi\rangle$ chosen such that set of permutations of $|\psi\rangle$
"as orthogonal as possible"

$$S_3 = \{s_i : i = 1..6\} = \{id,(12),(13),(23),(231),(312)\}$$

"Ideal" case: $\{s_i|\psi\rangle : i = 1..6\}$ orthogonal set

$$\sum_{i=1}^{6} s_i|\psi\rangle\langle\psi|s_i \cong \begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & 0 & \\ & & & & & & & 0 \end{pmatrix}$$

The p-f problem $|$  $\rangle + |$  $\rangle$

Quantum solution: $(\alpha^3 = 1)$

$$|\psi\rangle = \tfrac{1}{\sqrt{5}}|000\rangle + \sqrt{\tfrac{2}{15}}\left(|100\rangle + \alpha|010\rangle + \alpha^2|001\rangle\right) + \sqrt{\tfrac{2}{15}}\left(|110\rangle + \alpha^2|101\rangle + \alpha|011\rangle\right)$$

$|\psi\rangle$ chosen such that set of permutations of $|\psi\rangle$ "as orthogonal as possible"

$$S_3 = \{s_i : i = 1..6\} = \{id, (12), (13), (23), (231), (312)\}$$

"Ideal" case: $\{s_i|\psi\rangle : i = 1..6\}$ orthogonal set

$$\sum_{i=1}^{6} s_i|\psi\rangle\langle\psi|s_i \cong \begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & 0 & \\ & & & & & & & 0 \end{pmatrix}$$

However "cover" only 5 dimensions (not 6). $\langle s_i\psi | s_j\psi\rangle = \frac{1}{5}\delta_{ij}$

Why? Irreps of S_n in tensor-representation…

Basic facts from representation theory

Schur's lemma:

Let ρ be an irrep. of dimension d, A $\in$ GL(d) s.th.

$$A\rho(g) = \rho(g)A \quad \forall g \in G$$

then $A \cong I_d$.

Basic facts from representation theory

Schur's lemma:

Let ρ be an irrep. of dimension d, $A \in GL(d)$ s.th.

$$A\rho(g) = \rho(g)A \qquad \forall g \in G$$

then $A \cong I_d$.

Application: "group average" $A = \frac{1}{|G|}\sum_{g\in G}\rho(g)$

$$A\rho(g') = \frac{1}{|G|}\sum_{g\in G}\rho(g)\rho(g') = \frac{1}{|G|}\sum_{g\in G}\rho(gg') =$$

$$\frac{1}{|G|}\sum_{g\in G}\rho(g) = \frac{1}{|G|}\sum_{g\in G}\rho(g'g) = \frac{1}{|G|}\sum_{g\in G}\rho(g')\rho(g) = \rho(g')A$$

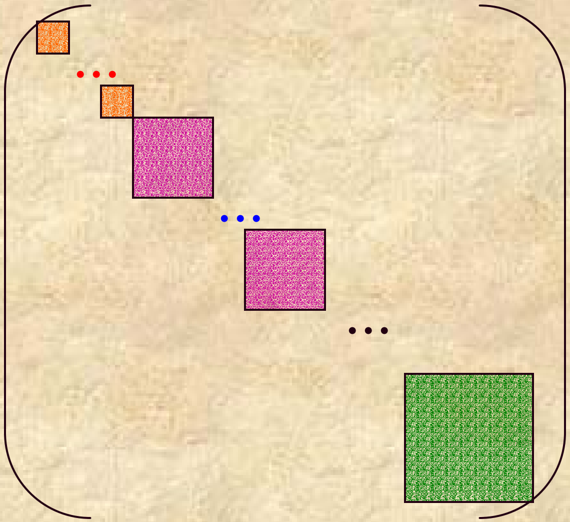
Representation Theory

S_n acts on $\mathbf{C}_k^{\otimes n}$ by permutation of the basis states

$\Rightarrow$ representation ρ in $GL(d^n)$

ex: $\rho((213))|101\rangle = |011\rangle$

splits space into irreducible subspaces V_ρ



$$s_\psi = \frac{1}{n!}\sum_{g\in S_n} \rho(g)|\psi\rangle\langle\psi|\rho^\dagger(g)$$

Note $\rho(g)s_\psi = s_\psi\rho(g) \quad \forall g \in S_n$

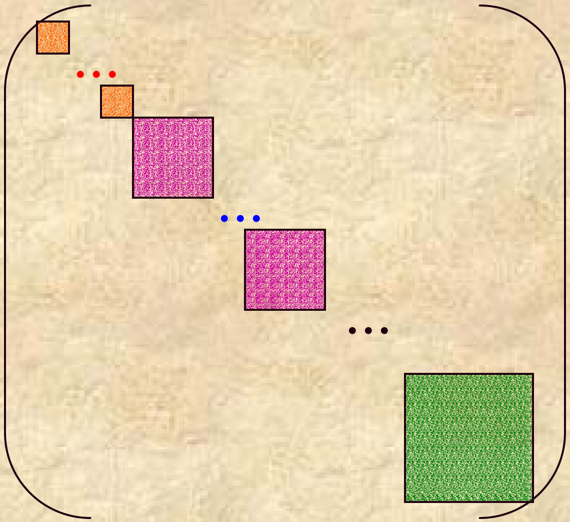
Representation Theory

S_n acts on $\mathbf{C}_k^{\otimes n}$ by permutation of the basis states

$\Rightarrow$ representation ρ in $GL(d^n)$

ex: $\rho((213))|101\rangle = |011\rangle$

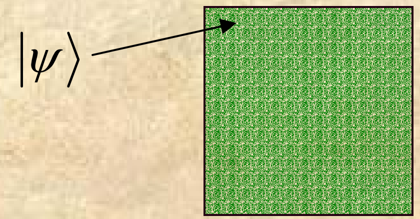
splits space into irreducible subspaces V_ρ



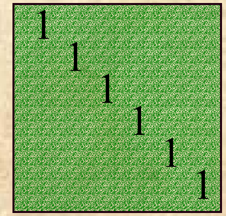
$$s_\psi = \frac{1}{n!}\sum_{g\in S_n} \rho(g)|\psi\rangle\langle\psi|\rho^\dagger(g)$$

Note $\rho(g)s_\psi = s_\psi \rho(g) \quad \forall g \in S_n$

Assume $|\psi\rangle \in V_\rho$. Then $s_\psi \cong Id$ by Schur's lemma



$s_\psi =$

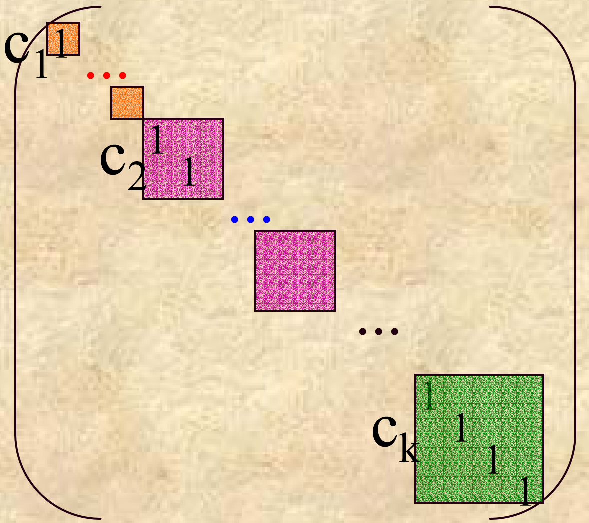


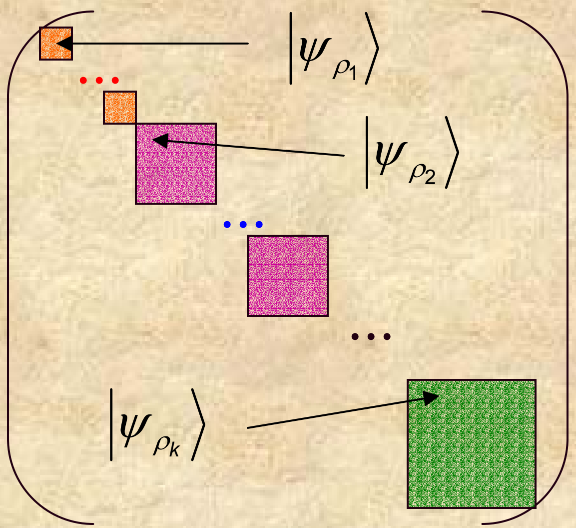
Representation Theory

If $|\psi\rangle = |\psi_{\rho_1}\rangle + |\psi_{\rho_2}\rangle + \ldots + |\psi_{\rho_k}\rangle$

Then

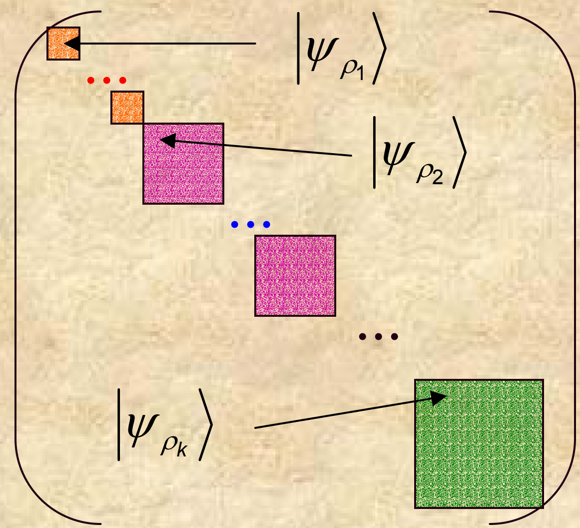
$s_\psi =$



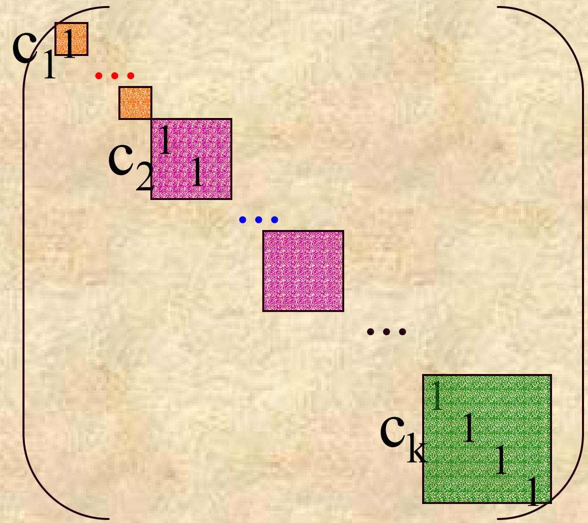


Representation Theory

If $|\psi\rangle = |\psi_{\rho_1}\rangle + |\psi_{\rho_2}\rangle + \ldots + |\psi_{\rho_k}\rangle$



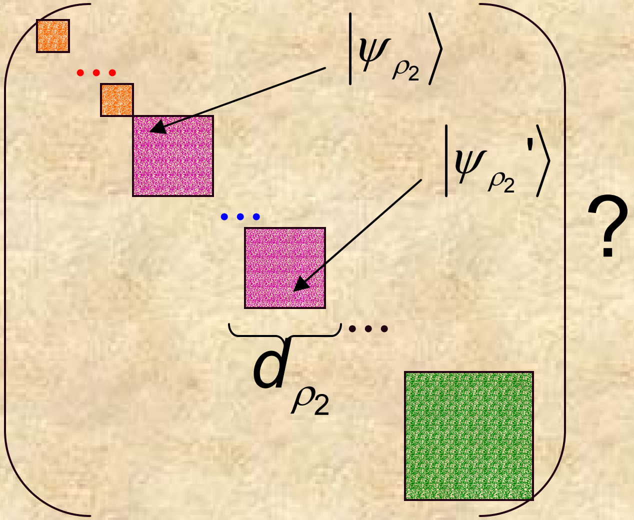
Then $s_\psi =$



Choose $|\psi\rangle = \frac{1}{\kappa}\left(\sqrt{d_{\rho_1}}|\psi_{\rho_1}\rangle + \sqrt{d_{\rho_2}}|\psi_{\rho_2}\rangle + \ldots + \sqrt{d_{\rho_k}}|\psi_{\rho_k}\rangle\right)$ to "cover" all space?

Problem: multiple equivalent irreps !

Representation Theory



Multiplicity of irrep ρ: m_ρ

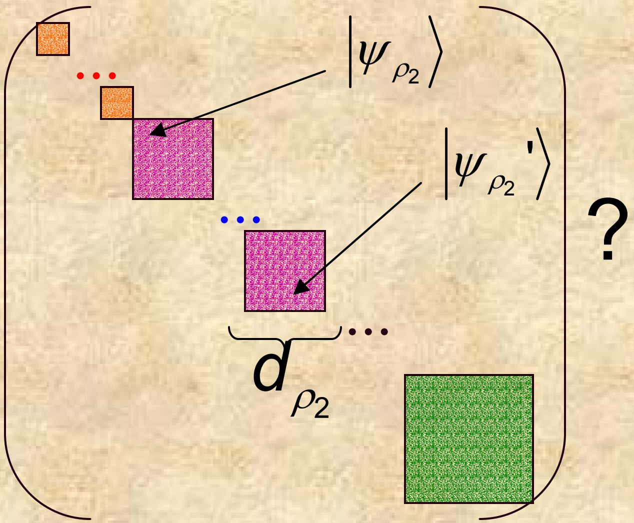
Can we "use" multiple copies of same irrep?

$$\sum_\rho m_\rho d_\rho = k^n$$

Result:

Th: Can use at most d_ρ copies of an irrep ρ.

Representation Theory



Multiplicity of irrep ρ: m_ρ

Can we "use" multiple copies of same irrep?

$$\sum_\rho m_\rho d_\rho = k^n$$

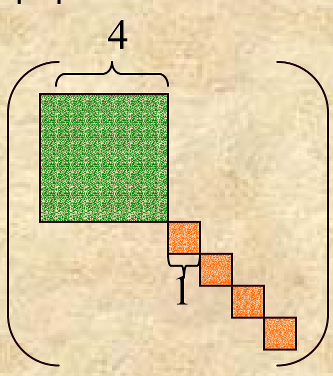
Result:

Th: Can use at most d_ρ copies of an irrep ρ.

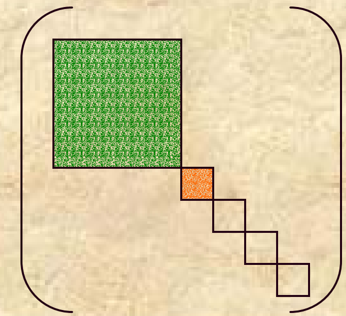
Ex.: S_3

$$\sum_{i=1}^{6} s_i |\psi\rangle\langle\psi| s_i \cong \begin{pmatrix} 1 &&&&&&& \\ & 1 &&&&&& \\ && 1 &&&&& \\ &&& 1 &&&& \\ &&&& 1 &&& \\ &&&&& 0 && \\ &&&&&& 0 & \\ &&&&&&& 0 \end{pmatrix}$$

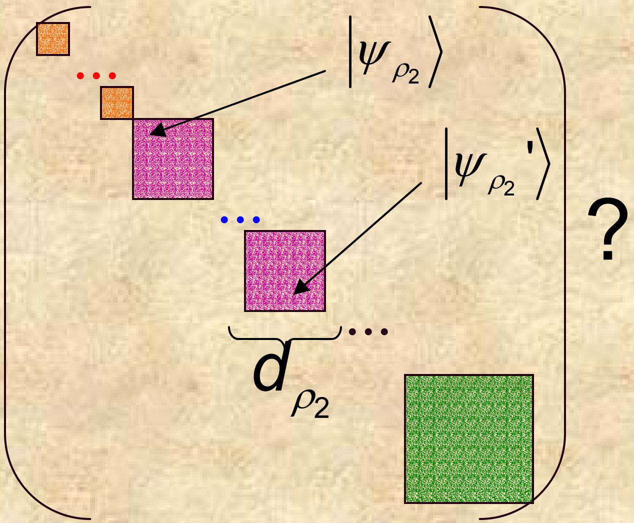
"cover" only 5 dim.



"use"



Representation Theory



Multiplicity of irrep ρ: m_ρ
Can we "use" multiple copies of same irrep?

$$\sum_{\rho} m_\rho d_\rho = k^n$$

Result:
Th: Can use at most d_ρ copies of an irrep ρ.

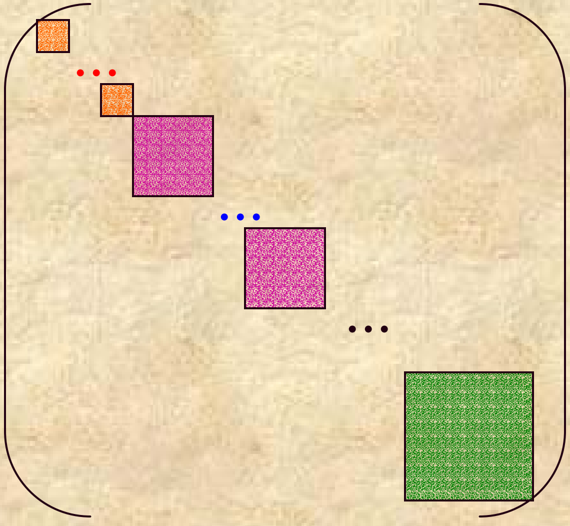
$$maxrank(s_\psi) = \sum_{\rho} \min(m_\rho, d_\rho) d_\rho$$

For $k \leq \frac{1}{5}\sqrt{n}$ **"most" irreps have multiplicity smaller than their dimension. "Loose" only o(k^n) part of full space.**

The p-f problem

Use Young-tableau rules to estimate

$m_{max} \leq n^{k^2}$, number of irreps of S_n at most $\binom{n}{k}$



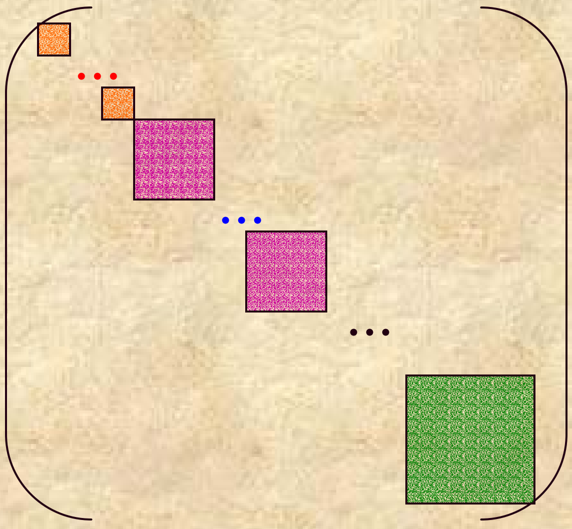
$$\sum_\rho m_\rho d_\rho = k^n$$

$$\max rank(s_\psi) = \sum_\rho \min(m_\rho, d_\rho) d_\rho$$

$$\geq k^n - \sum_{\rho : m_\rho > d_\rho} (m_\rho - d_\rho) d_\rho \geq k^n - \sum_{\rho : m_\rho > d_\rho} m_\rho m_\rho \geq k^n - \binom{n}{k} n^{2k^2}$$

$$= k^n - o(k^n) \qquad k < \frac{1-\varepsilon}{4}\sqrt{n}$$

Summary



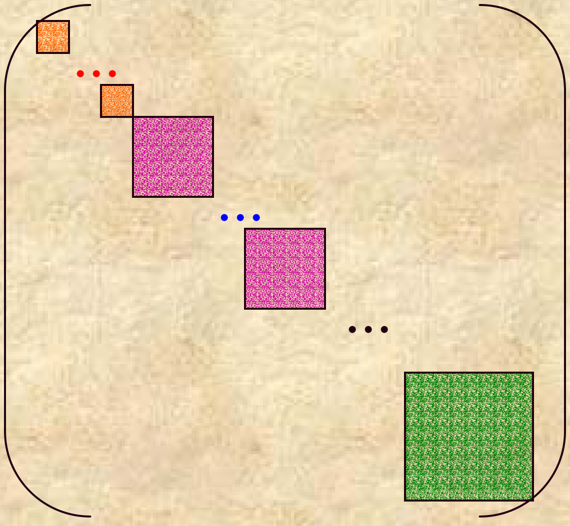
Permutation transmission:

• quantum advantage to transmission of permutation through a shuffling channel
• less colors needed quantumly

HSP:

• identified large class of hidden subgoups of S_n that cannot be distinguished from each other
• evidence that QFS (with random basis) not stronger than classical search for S_n

Open Questions



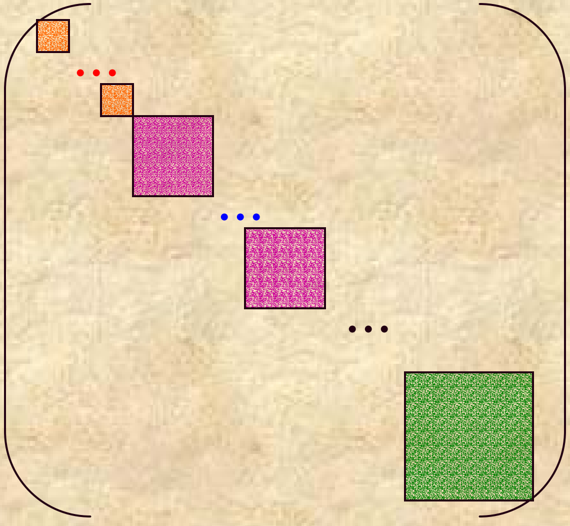
Permutation transmission:

- Prove result for all k (probably true)
  (⇒ ≈n/e colors for p = 1)
- find more applications, also for other groups

HSP:

- Prove group theoretic conjecture
- Prove there is no “good” basis for the strong method

Open Questions



Permutation transmission:

• Prove result for all k (probably true)
  ($\Rightarrow \approx n/e$ colors for $p = 1$)
• find more applications, also for other groups

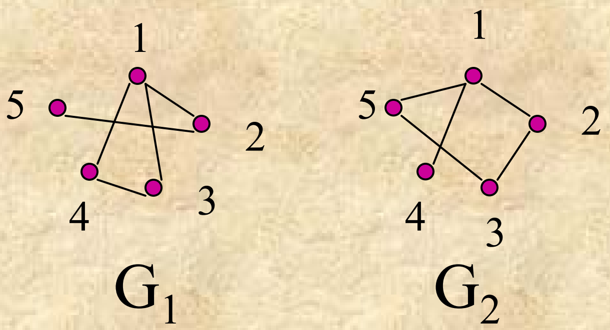
HSP:

• Prove group theoretic conjecture
• Prove there is no “good” basis for the strong method

~~QFS for HSP~~

STOP!!!

Graph Isomorphism



$G_1 \approx G_2$?

Let $G = G_1 \cup G_2$ and determine automorphism group

$A = \{\pi \in S_{2n} : \pi(G) = G\}$.

Check if it splits as $H_1 \times H_2 \subseteq S_n \times S_n$ ($\Rightarrow G_1 \not\approx G_2$).

A is hidden subgroup of S_n of $f: S_n \rightarrow G$

$f: \pi \rightarrow \pi(G)$