

Distinguishability of states

\mathcal{H} : n dim. complex Hilbert-space

set of states: $S(\mathcal{H}) = \{ \rho \in \text{Lin}(\mathcal{H}) \mid \rho \geq 0, \text{Tr}(\rho) = 1 \}$

a measurement with k possible outcomes:

a partition of unity $E_1, \dots, E_k \geq 0, E_1 + \dots + E_k = I$ in the sense that

if system is in state $\rho \in S(\mathcal{H})$ (when the measurement is performed)

then $P(\text{"outcome is } j\text{"}) = \text{Tr}(\rho E_j)$

Def.: the collection $\rho_1, \dots, \rho_k \in S$ is dist. w. certainty when

$\exists E_1, \dots, E_k$ partition of unity s.t. $\#_{j=1, \dots, k} : \text{Tr}(\rho_j E_j) = 1$

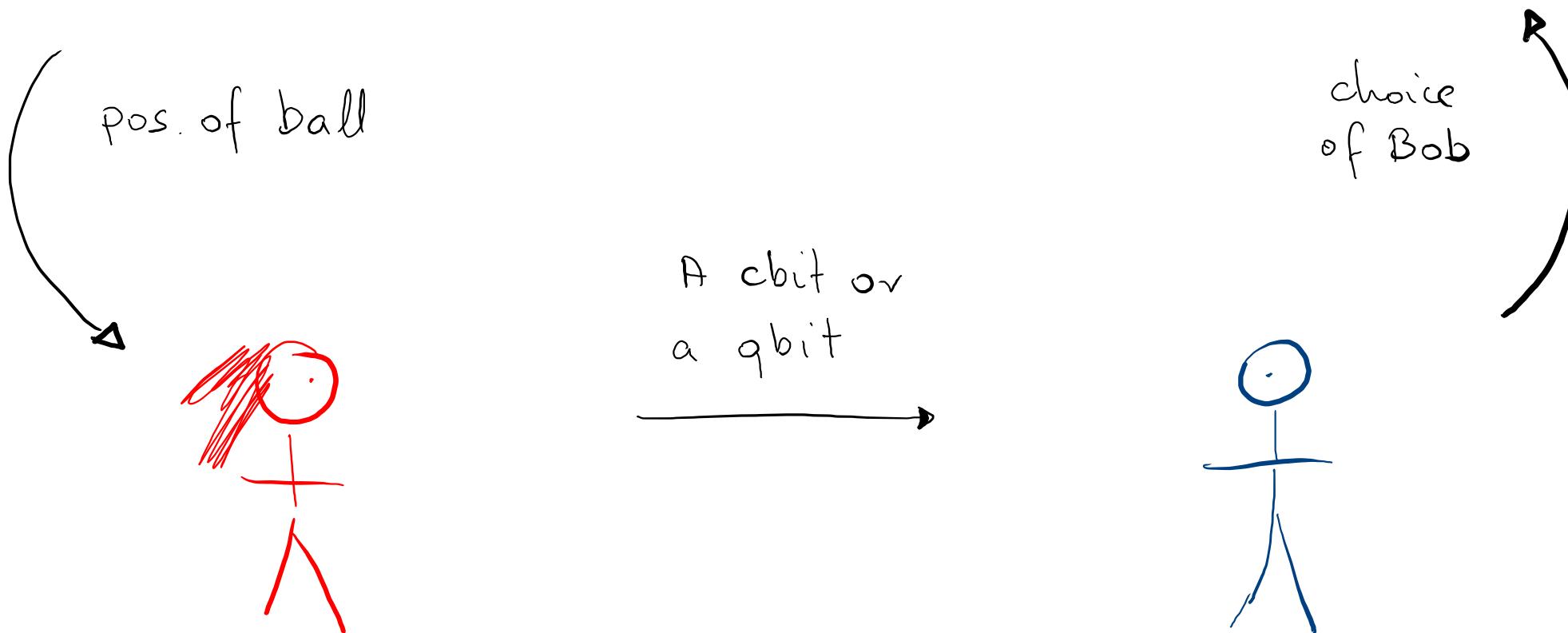
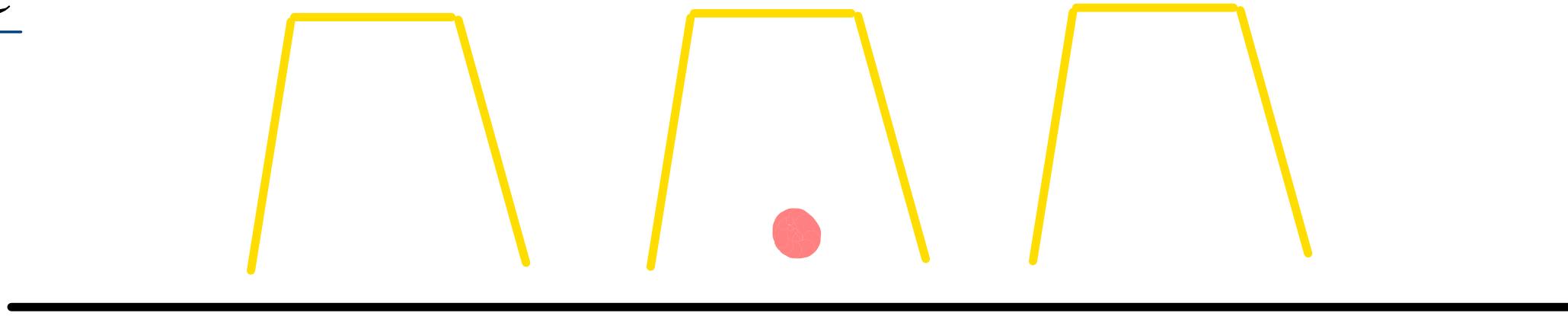
Prop.: the collection $\rho_1, \dots, \rho_k \in S$ is dist. w. certainty



$\forall j \neq l : \text{Im } \rho_j \perp \text{Im } \rho_l$

Cor.: the max. cardinality of a coll. of states that can be dist. w. certainty is $n = \dim(\mathcal{H})$.

A game



Using a cbit, max. $p(\text{win}) = \frac{2}{3}$.

Q.: What is max. $p(\text{win})$ if they use a qbit?

Strategy = encoding + decoding

Encoding: $\beta_1, \beta_2, \beta_3 \in S(\mathbb{C}^2)$

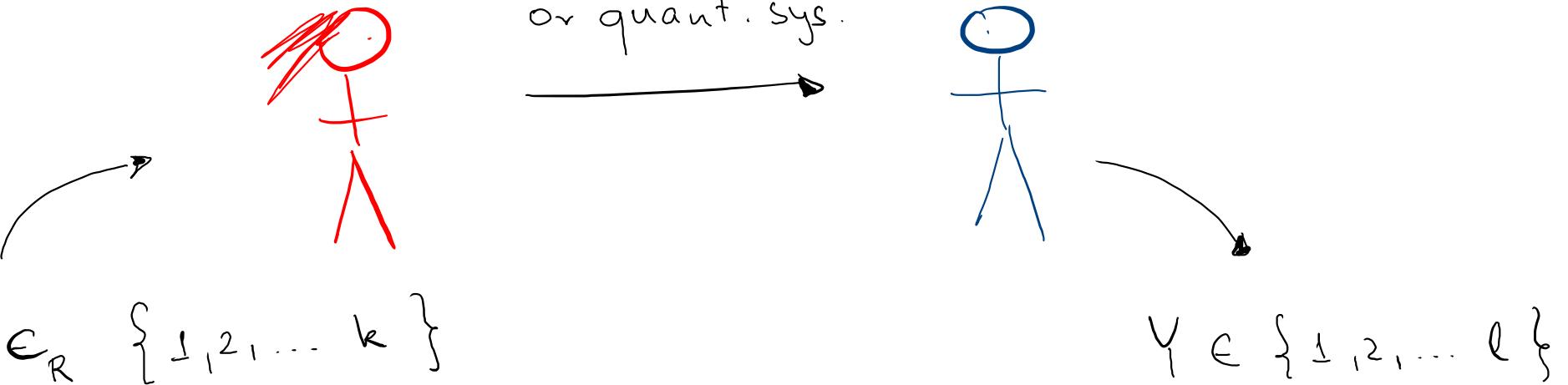
Decoding: E_1, E_2, E_3 part. of unity

$$p(\text{win}) = \frac{1}{3} \text{Tr}(\beta_1 E_1) + \frac{1}{3} \text{Tr}(\beta_2 E_2) + \frac{1}{3} \text{Tr}(\beta_3 E_3)$$

$$\leq \frac{1}{3} \text{Tr}(E_1) + \frac{1}{3} \text{Tr}(E_2) + \frac{1}{3} \text{Tr}(E_3) = \frac{1}{3} \text{Tr}(I) = \frac{2}{3}$$

nnn	aaa	aa.	aaa
nnn	$\text{Tr}(\beta_1 E_1)$	$\text{Tr}(\beta_2 E_1)$...
nnn	$\text{Tr}(\beta_1 E_2)$
nnn

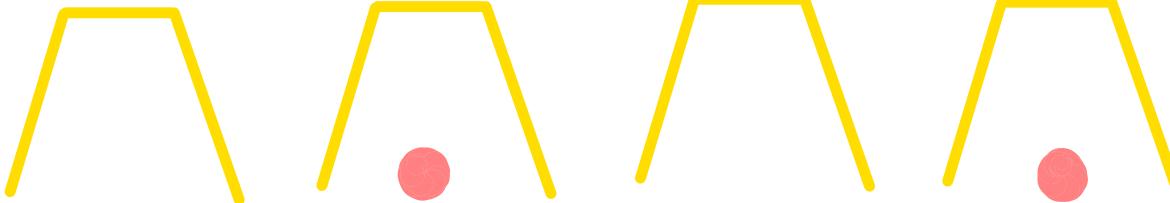
Game type



- reward = $R(X, Y)$
- the prob. dist. of X and the reward-func. R is public
- aim: achieve highest $E(\text{reward})$

We'll see: in this game type quantum does not give an advantage over classical

Further example of a game of this type:



"4 cups, 2 balls game"

pos. of the 2 balls



1 cbit or qbit



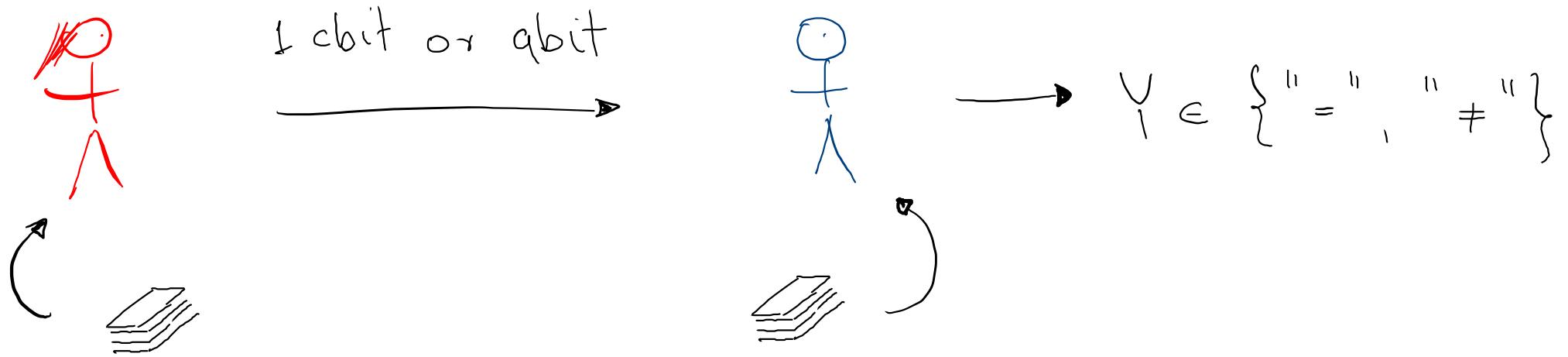
choice of
a single
cup

- all 6 possible arrangement with equal prob.

- Reward = 1\$ if Bob finds a ball, 0\$ otherwise

$$\begin{aligned} \text{with 1 cbit} \\ \max \mathbb{E}(\text{reward}) \\ = \max p(\text{win}) \\ = 1 \cdot \frac{1}{6} = \frac{5}{6} \end{aligned}$$

A game which is not of the mentioned type



$$X_1 \in_R \{ "A", "B", "C" \} \supseteq X_2$$

- X_1, X_2 are drawn in a uniform & indep. manner
- win : when $X_1 Y X_2$ is true

Using a classical bit : $\max p(\text{win}) = \frac{5}{9} + \frac{1}{2} \cdot \frac{4}{9} = \frac{7}{9}$

Using a q. bit ? Strategy:

Encoding : $S_A, S_B, S_C \in S(\mathbb{C}^2)$

Decoding : 3 part. of unity (dep. on the value of X_2) :

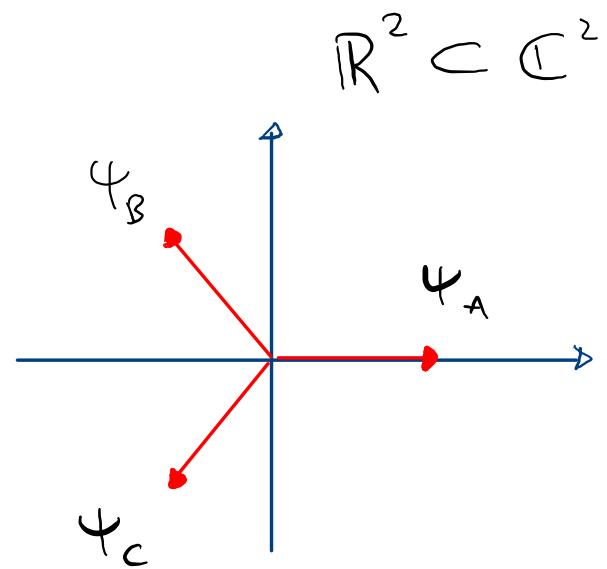
$$E_{=}^A, E_{\neq}^A$$

$$E_{=}^B, E_{\neq}^B$$

$$E_{=}^C, E_F^C$$

$$\hookrightarrow p(\text{win}) = \frac{1}{9} \left(\text{Tr} \left(S_A E_{=}^A \right) + \text{Tr} \left(S_A E_{\neq}^B \right) + \dots \right)$$

E.g.



$$S_x := |\varphi_x \times \varphi_x|$$

$$E_x^+ := S_x, \quad E_x^- := I - S_x$$

→ $P(\text{win}) = \frac{1}{9} \left(3 \cdot 1 + 6 \cdot \frac{3}{4} \right) = \frac{5}{6} > \frac{7}{9}$!

Back to our chosen gametype

An actual strategy (encoding + decoding) fixes the input-output (or channel) matrix $T_{i,j} = p(Y=i | X=j)$.

$\mathbb{E}(\text{reward}) = \sum_{i,j} R(i,j) T_{i,j} p(X=j)$ is a lin. functional of the channel matrix (i.e. taking convex combinations - or physically: allowing the use of a common source of randomness - does not help). So consider the sets

$$Q_n(k,l) := \text{Conv.} \left\{ \left(\text{Tr} (S_j E_i) \right)_{i,j} \mid \begin{array}{l} S_1, \dots, S_k \in S(\mathbb{C}^n) \\ E_1, \dots, E_l \text{ is a part. of unity} \end{array} \right\}$$

$$C_n(k,l) := \text{Conv.} \left\{ \left(T_{i,j} \right)_{i,j} \mid T_{i,j} \geq 0, \sum_i T_{i,j} = 1, T \text{ has at most } n \text{ nonzero rows} \right\}$$

- $C_n(k,l)$ is convex
 - $C_n(k,l) \subset Q_n(k,l)$
 - $E(\text{reward}) = \sum_{i,j} R(i,j) T_{i,j} P(X=j)$
is an arbitrary lin. functional
of the channel matrix
- } \nexists a game of the specified type where quantum gives an advantage over classical iff $\nexists_{n,k,l}$:
 $Q_n(k,l) = C_n(k,l)$

→ The task is to show: $Q_n(k,l) = C_n(k,l)$

Note : suppose $T_{i,j} = \text{Tr}(S_i E_j)$ for some $S_1, \dots, S_k \in S(\mathbb{C}^n)$
 E_1, \dots, E_n part. of unity. $\begin{pmatrix} \cdot & \circ & \cdot \\ \cdot & \cdot & \circ \\ \cdot & \circ & \cdot \end{pmatrix}$

$$\sum_j T_{j, f(j)} = \sum_j \text{Tr}(S_{f(j)} E_j) \leq \sum_j \text{Tr}(E_j) = \text{Tr}(I) = n$$

$$\hookrightarrow \text{with } Q_n(k, l) := \left\{ (T_{i,j})_{i,j} \mid \begin{array}{l} T_{i,j} \geq 0, \sum_j T_{i,j} = 1 \\ \forall f: \sum_j T_{j, f(j)} \leq n \end{array} \right\}$$

we have : $C_n(k, l) \subset Q_n(k, l) \subset \Omega_n(k, l)$.

e.g. $C_2(3, 3) = \Omega_2(3, 3)$ immediately implying that

$$C_2(3, 3) = Q_2(3, 3) = \Omega_2(3, 3)$$

However :

$$T := \begin{pmatrix} & \text{0000} & \text{0001} & \text{0010} & \text{0011} & \text{0100} & \text{0101} \\ & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 \\ & \frac{1}{2} & 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} & \frac{1}{2} \end{pmatrix} \in \Omega_2(6,4)$$

but with this channel matrix the "4 cups, 2 balls game" could be won with prob 1! $\Rightarrow T \notin C_2(6,4)$

↳ $C_2(6,4) \neq \Omega_2(6,4)$; the "triv." inequalities are not enough to show that $\Omega_2(6,4)$ coincides with $C_2(6,4)$

GPT setting

- state space : S convex set

(„mixing“ is physically well-defined : $\circ \circ \circ \circ \dots \circ$)

- set of all measurements

A measurement with k possible outcomes:

$$M: S \xrightarrow{\text{affine}} \text{Simplex}_k = \left\{ (t_1 \dots t_k) \in \mathbb{R}^k \mid t_1, t_2, \dots, t_k \geq 0, \sum_{j=1}^k t_j = 1 \right\}$$

$$\text{s.t. } M(\lambda s + (1-\lambda)\sigma) = \lambda M(s) + (1-\lambda)M(\sigma) \quad \forall s, \sigma \in S, \lambda \in [0,1]$$

pick one in a random manner and forget the label

$S = S(\mathcal{A})$:

$M : S \rightarrow \text{Simplex}_k$ is an affine map



$$M(s) = (\text{Tr}(sE_1), \dots, \text{Tr}(sE_k)) \text{ where } E_1, \dots, E_k \geq 0, E_1 + \dots + E_k = I$$

$S = \text{Simplex}_n$:

$M : S \rightarrow \text{Simplex}_k$ is an affine map



$$M(s) = t_1 q_1 + t_2 q_2 + \dots + t_n q_n \text{ where } q_1, \dots, q_n \in \text{Simplex}_k$$

The set of all measurements should satisfy some physical requirements ; it cannot be arbitrarily small !

Both in the q. and c. case , the set of all measurements is simply the set of all $S \rightarrow \text{Simplex}$ affine maps .

So in our GPT model we shall assume :

- state space is a given S convex set
- any $S \xrightarrow{\text{affine}} \text{Simplex}_*$ map is a realizable measurement
(measurements are precisely these maps)

Then the convex geo. of the state space S completely determines the set of input-output matrices one can realize by using this system with some **encoding** and **decoding** proc. for (classical) inf. storage.

$$\text{Ch}_S(k, l) := \text{Conv.} \left\{ \left(\mu_j(s_i) \right)_{i,j} \mid M: S \xrightarrow{\text{affine}} \text{Simplex}_l \right\}$$

$s_1, s_2 \dots s_k \in S$

We have $Q_n = \text{Ch}_{S(\mathbb{C}^n)}$, $C_n = \text{Ch}_{\text{Simplex}_n}$

Measures of inf. storage capacities

- syst. with state space S can be used to simulate (for class. inf. storage) another syst. with state space \tilde{S} :

$$\forall k, l : \text{Ch}_S(k, l) \supseteq \text{Ch}_{\tilde{S}}(k, l)$$

- $\Delta(S) := \max \{ n \mid S \text{ can simulate Simplex}_n \}$
 $\equiv \max \{ n \mid \exists s_1, \dots, s_n \in S : s_1 \dots s_n \text{ can be dist. w. certainty} \}$

- $d(S) := \min \{ n \mid S \text{ can be simulated by Simplex}_n \}$
"signalling dimension" of S

- $$st(S) := \sup \left\{ Tr(T) \mid k \in \mathbb{N}, T \in Cl_S(k,k) \right\}$$

$$= \left\{ \sum_{j=1}^k M_j(s_j) \mid k \in \mathbb{N}, s_1 \dots s_k \in S, M : S \rightarrow \text{Simplex}_k \right\}$$

"storage-capacity of Matsumoto and Kimura"

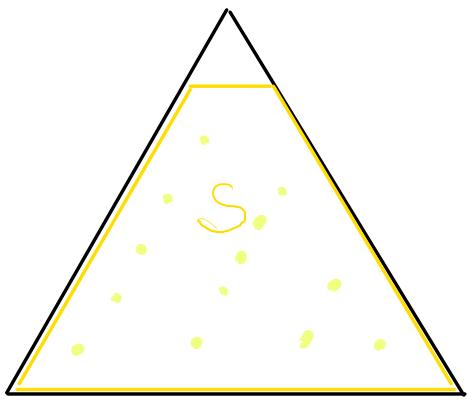
Clear:

- $S(\mathbb{C}^n)$ can simulate Simplex_n
- if $S = \text{Simplex}_n$, then $\Delta(S) = st(S) = d(S) = n$
- $\Delta(S) \leq st(S) \leq d(S)$
- $\Delta(S(\mathbb{C}^n)) = st(S(\mathbb{C}^n)) = n$

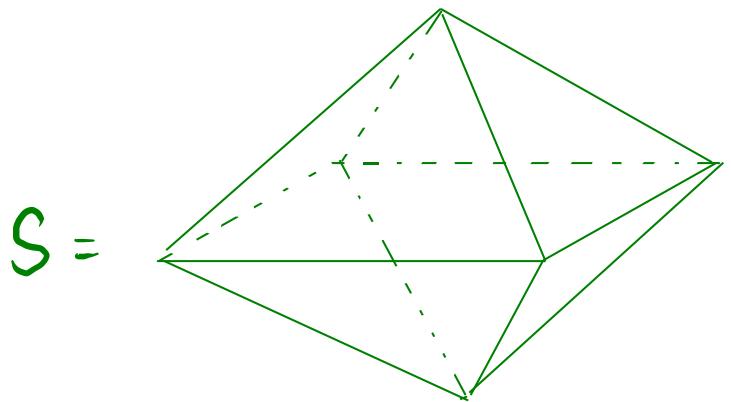
Less clear, but true :

- $st(S) = (\text{Minkowski-degree of asymmetry of } S) + 1$
(Matsumoto & Kimura)
- $d(S(C^n)) = n$ (Frinkel & Weiner)
- in general, all of these quantities (Δ, st, d)
are different

Examples



$$\Rightarrow \Delta(S) = 2, \text{ but } st(S) \geq 3 - \varepsilon$$



$$\Rightarrow st(S) = 2 \quad (\text{b.c. of central-symmetry})$$

$$\text{but } T = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} & \frac{1}{2} \end{pmatrix} \in \text{Ch}_S(G, 4)$$

$$\Rightarrow d(S) > 2$$