§ 3 The illustrated guide to point games

Goal: (1) Basic Moves
(2) Describe simple protocols $\epsilon = 1/\sqrt{2} - 1/2$ & $\epsilon = 1/6$

Recall: $[z]$, $[x, y]$, $\sum p_i(z) f(z) \leq \sum p_{i+1}(z) f(z)$ $\forall f \in$ op. mon.

§ 3.1 Basic Moves

Motiv^n: All non-trivial one-variable transitions: $1 \to 1$, $2 \to 1$, $1 \to 2$

NB: (claim) (1) These generate all $1 \to n$ & $n \to 1$ transititions.

(2) Not a complete basis; Many $2 \to 2$ moves not covered.

§ 3.1.1 Point Raising

$$p[z] \to p[z']$$

valid iff $p f(z) \leq p f(z')$
(already imposed prob. conservation)

claim: $z \leq z'$ $\Leftrightarrow$ $f(z) \leq f(z')$ $\forall f$.

⌈proof: $z \leq z' \Rightarrow f(z) \leq f(z')$ by def^n of f.
$f(z) \leq f(z')$
$\Rightarrow f(z) = z$ also satisfies. ⌋

NB: Extra unmoving points don't matter

$$p[z] + \sum_i \underset{\substack{\uparrow \\ \geq 0}}{p_i} \underbrace{[z_i] \to p[z'] + \sum_i p_i [z_i]}_{\text{unmoving}}$$

remark: Can always move away.

§ 3.1.3 Point Splitting

$$(p_1 + p_2)[z] \to p_1[z_1'] + p_2[z_2']$$

most general form

NB: Prob cons. imposed; $p_1 > 0$ $p_2 > 0$ assumed.

Recall: Valid $\leftrightarrow$ $(p_1+p_2) f(z) \leq p_1 f(z_1') + p_2 f(z_2')$

$f(z) = 1 \leftrightarrow$ prob. ✓

$f(z) = \frac{\lambda z}{\lambda + z} = \lambda\left(1 - \frac{\lambda}{\lambda+z}\right) \overset{\text{works}}{\Longleftrightarrow} f(z) = -\frac{1}{\lambda+z}$

$(f(z) = z$ when $\lambda \to \infty)$

For $z \neq 0$, $\lambda = 0 \Rightarrow$

$$\frac{-p_1+p_2}{z} \leq -\frac{p_1}{z_1'} - \frac{p_2}{z_2'}$$

claim: $\Leftrightarrow$ valid.

proof: obviously if $(p_1+p_2) f(z) \leq p_1 f(z_1') + p_2 f(z_2')$

$\Rightarrow \frac{-(p_1+p_2)}{z} \leq -\frac{p_1}{z_1'} - \frac{p_2}{z_2'}$ (as above).

If $-\frac{(p_1+p_2)}{z} \leq -\frac{p_1}{z_1'} - \frac{p_2}{z_2'} \overset{\text{(will show)}}{\Rightarrow}$ holds for $f(z) = \frac{-1}{\lambda+z}$

(rest follows).

Take $\frac{1}{z} = w$. The constraint with $f(z) = \frac{-1}{\lambda+z}$ will

be $\frac{-(p_1+p_2)}{\lambda + \frac{1}{w}} \leq \frac{-p_1}{\lambda + \frac{1}{w_1'}} - \frac{p_2}{\lambda + \frac{1}{w_2'}}$.

claim: This is $(p_1+p_2) g(w) \leq (p_1+p_2)\, g\left(\frac{p_1 w_1' + p_2 w_2'}{p_1+p_2}\right)$

$\leq p_1 g(w_1') + p_2 g(w_2')$

for $g(w) = -\frac{w}{w\lambda+1}$ $\left(= \frac{-1}{\lambda + \frac{1}{w}} \right)$

proof:

NB: $g(w)$ is monotonically decr. $w\uparrow$ den $\downarrow$ $(-g)\uparrow$

NB 2: $w(p_1+p_2) \geq p_1 w_1' + p_2 w_2'$

$w \geq \frac{p_1 w_1' + p_2 w_2'}{p_1+p_2}$

$\Rightarrow$ 1st ineq.

NB 3: $g(w)$ is convex.

§ 3.1.2 *Point Merging*

$$p_1[z_1] + p_2[z_2] \to (p_1+p_2)[z']$$

valid $\Leftrightarrow$ $p_1 f(z_1) + p_2 f(z_2) \leq (p_1+p_2) f(z')$ $\forall f$ op. mon.

$\Rightarrow$ for $f(z) = z$,

$$\frac{p_1 z_1 + p_2 z_2}{p_1+p_2} \leq z'$$

claim: $\dfrac{p_1 z_1 + p_2 z_2}{p_1+p_2} \leq z' \Leftrightarrow$ valid.

$\lceil$ proof: NB: $f(z) = \dfrac{\lambda z}{\lambda + z}$ is concave.

i.e. $f(\theta z_1 + (1-\theta) z_2) \geq \theta f(z_1) + (1-\theta) f(z_2)$

let $\theta = \dfrac{p_1}{p_1+p_2}$.

$$\Rightarrow f\left(\frac{p_1 z_1 + p_2 z_2}{p_1+p_2}\right) \geq \frac{p_1 f(z_1) + p_2 f(z_2)}{p_1+p_2}$$

From monotonicity & using $\dfrac{p_1 z_1 + p_2 z_2}{p_1+p_2} \leq z'$

$$(p_1+p_2) f(z') \geq p_1 f(z_1) + p_2 f(z_2)$$

$\lfloor$

similarly $p_1[x_1, y] + p_2[x_2, y] \to (p_1+p_2)\left[\dfrac{p_1 x_1 + p_2 x_2}{p_1+p_2}, y\right]$

NB: $0.5[0,0] + 0.5[1,1] \to 1[0.5, 0.5]$ is NOT valid.

Remark: Strong coin flipping impossibility is

$0.5[0,0] + 0.5[1,1] \to 1[z,z]$ is

transitively invalid if $z < 1/\sqrt{2}$.

§ 3.1.4 Summary

Lemma 20.

- Point raising $\quad p[z] \to p[z'] \quad$ (for $z \le z'$)
- Point merge $\quad p_1[z_1] + p_2[z_2] \to (p_1+p_2)\left[\frac{p_1 z_1 + p_2 z_2}{p_1+p_2}\right]$
- Point split $\quad (p_1+p_2)\left[\frac{p_1+p_2}{p_1 w_1' + p_2 w_2'}\right] \to p_1\left[\frac{1}{w_1'}\right] + p_2\left[\frac{1}{w_2'}\right]$

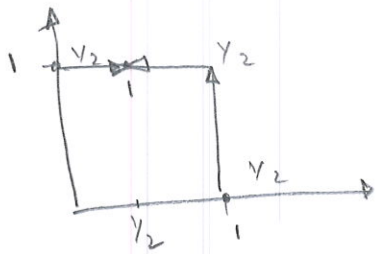
§ 3-2 Basic Protocols

(1)(a) Protocol stupid: One player flips (say Alice) & announces the result.

claim: $\frac{1}{2}[1,0] + \frac{1}{2}[0,1] \to \frac{1}{2}[1,1] + \frac{1}{2}[0,1]$

$$\downarrow$$

$$1\left[\tfrac{1}{2}, 1\right]$$



NB: First non-trivial message is sent by Alice

$\Updownarrow$ (Recall: reverse time convention)

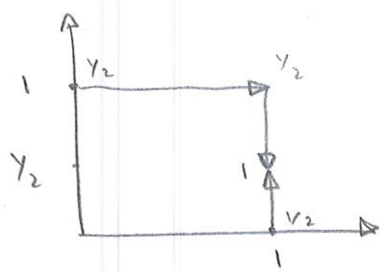
Last transition is horizontal.

(b) Protocol Stupid 2: Bob tosses & announces the result.

claim: $\frac{1}{2}[1,0] + \frac{1}{2}[0,1] \to \frac{1}{2}[1,0] + \frac{1}{2}[1,1]$

$$\downarrow$$

$$1\left[1, \tfrac{1}{2}\right]$$



§ 3.2.1 The Spekkens & Rudolph protocol.

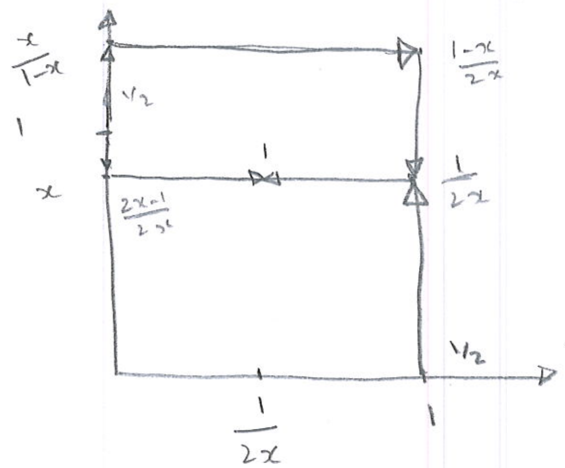
Fix $x \in (1/2, 1)$.

$$\frac{1}{2}[1,0] + \frac{1}{2}[0,1] \xrightarrow{\text{split}} \frac{2x-1}{2x}[x,0] + \frac{1-x}{2x}\left[\frac{x}{1-x},0\right] + \frac{1}{2}[0,1]$$

$$\xrightarrow{\text{raise}} \frac{2x-1}{2x}[x,0] + \frac{1-x}{2x}\left[\frac{x}{1-x},1\right] + \frac{1}{2}[0,1]$$

$$\xrightarrow{\text{merge}} \frac{2x-1}{2x}[x,0] + \frac{1}{2x}[x,1]$$

$$\xrightarrow{\text{merge}} 1\left[x,\frac{1}{2x}\right]$$



NB: $P_B^* = x$, $P_A^* = \frac{1}{2x}$ $\Rightarrow$ $P_A^* P_B^* = \frac{1}{2}$ (the trade off curve)

Remark: Clever step was a split before merging.

First step $\longleftrightarrow$ Last step ; cheat detection step.
TDPG protocol

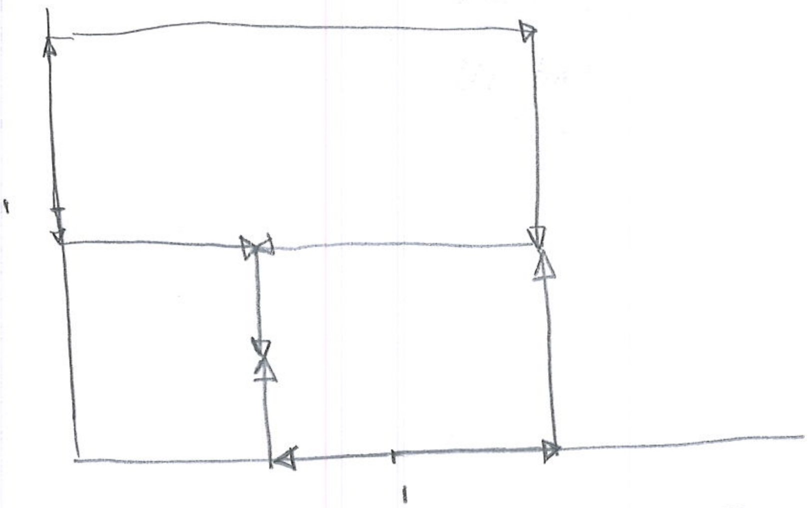
Remark 2: The avg. value of x & y can't decrease in any move ($\because$ observe the moves
or $\because$ $f(z)=z$ is operator mon; same thing)
$\therefore$ A perfect zero bias protocol would never increase these averages.
$\therefore$ Here we have 2 "bad" steps: split (increases avg y)
: raise (increases x).

$\therefore\ P_A^* = P_B^* = \frac{1}{2}$ balances the badness.

why? not clear (yet?)

§ 3.2.2 Quantum Public-coin Protocols

Improved Prot^l:

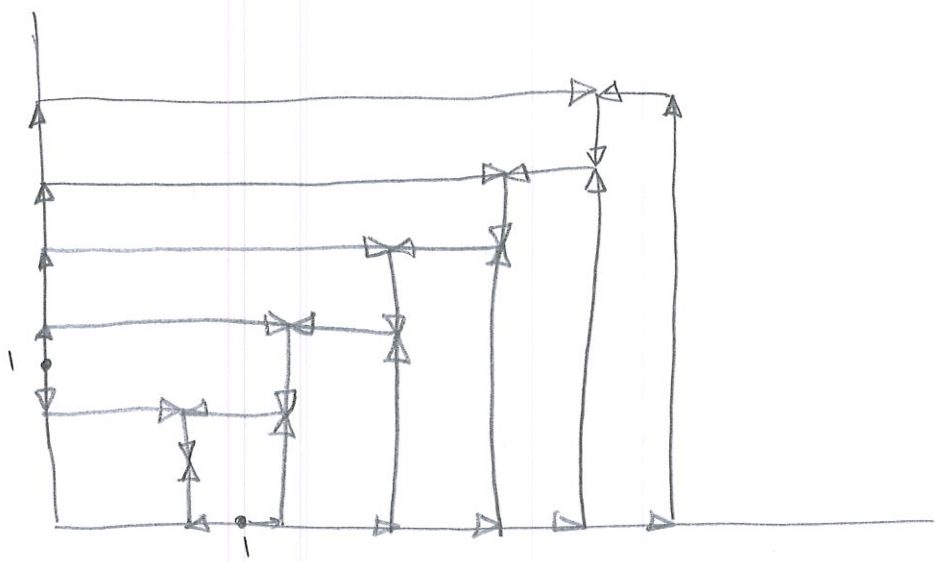


Remark: Structure of new protocol : Struct of Spekkens

$\parallel$

Struct. of Spekkens : Struct. of stupid

Iterated Prot^l:



Question: The best bias?

Answer (claim):
In the limit of infinite points, $1/6$ is the best bias "achievable".

Proof: Imagine we've split initially into so many points that we describe their prob. using a continuous prob density

The initial state then, is

$$\frac{1}{2}\int_{z^*}^{\infty} p(z)\,[z,0]\,dz + \frac{1}{2}\int_{z^*}^{\infty} p(z)\,[0,z]\,dz$$

with $\int_{z^*}^{\infty} p(z)\,dz = 1$. $z^* > 0$ is the point before which there are no points.

Remark: In the contin limit, the process is that of a point moving along the diagonal; it starts at (∞,∞) with zero prob. & collects prob. as it moves down, ending at $[z^*, z^*]$ with all the prob.

Idea: For what $p(z)$ is this possible?

$\Updownarrow$

for what $p(z)$ is

$$\frac{1}{2}\int_{z^*}^{\infty} p(z)\,[z,0]\,dz + \frac{1}{2}\int_{z^*}^{\infty} p(z)\,[0,z]\,dz$$

$\downarrow$

$$1\,[z^*, z^*]$$

transitively valid?

Sol^n: Let $Q(z)$ be the prob. traveling along the diagonal.

$$Q(z)\,[z,z] \rightarrow Q(z-dz)\,[z-dz, z-dz]$$

can be achieved as

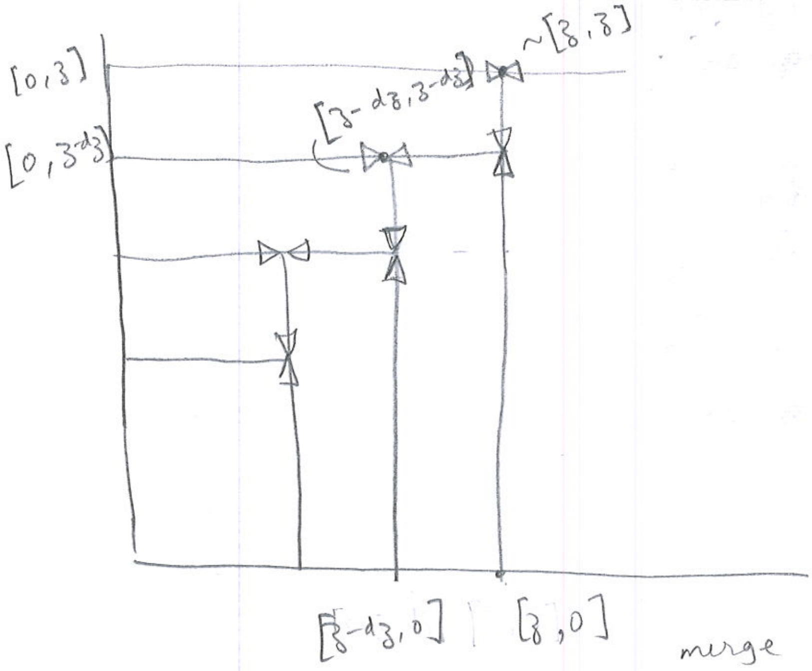
$$Q(z)\,[z,z] \xrightarrow{\text{merge}} \left(Q(z) + \frac{p(z)\,dz}{2}\right)[z, z-dz]$$

$$+ \qquad\qquad\qquad\qquad +$$

$$\frac{1}{2}\int_{z^*}^{z-dz} p(z)\,dz\,([0,z]+[z,0]) \qquad \frac{1}{2}\int_{z^*}^{z-dz} p(z)\,dz\,([0,z]+[z,0])$$

$$+\ \frac{1}{2}p(z)\,dz\,[z,0]$$

(see figure)



merge

$$\left(Q(z) + \frac{p(z)}{2}dz\right)[z, z-dz] + \frac{1}{2}p(z)dz[0, z-dz]$$

$$+ \frac{1}{2}\int_{z^\alpha}^{z-2dz} p(z)\,dz\left([0,z] + [z,0]\right) + \frac{1}{2}p(z)\,dz\,[z-dz, 0] \longrightarrow$$

$$\left(Q(z) + p(z)\,dz\right)[z-dz, z-dz] + \left(\frac{1}{2}\int_{z^\alpha}^{z-2dz} p(z)dz\left([0,z]+[z,0]\right)\right.$$

$$\left. + \frac{1}{2}p(z)\,dz\,[z-dz, 0]\right)$$

$\shortparallel$ demand

$$Q(z-dz)\quad [z-dz, z-dz] + \left(\;\cdots\cdots\right)$$

$$\Rightarrow\quad Q(z-dz) = Q(z) + p(z)\,dz$$

$$\Rightarrow\quad \boxed{\frac{dQ}{dz} = -p}$$

Further, point merges should preserve average coordinates.
(recall the constraints on point merge $p_1[z_1] + p_2[z_2] \rightarrow p_1+p_2\left[\frac{p_1 z_1 + p_2 z_2}{p_1+p_2}\right]$)

$$z - dz = \frac{Q(z)(z) + \frac{1}{2}p(z)\,dz\,(0)}{Q(z) + \frac{1}{2}p(z)\,dz} \Rightarrow \cancel{Qz} - Q\,dz + \frac{1}{2}pz\,dz - \frac{1}{2}p\,dz\,dz = \cancel{Qz}$$

$$\Rightarrow \boxed{Q = \frac{1}{2}pz}$$

Combining
$$\frac{dQ}{dz} = \frac{-2Q}{z}$$

NB: We haven't used point splitting constraints, nor prob. consⁿ.

$Q = \frac{c}{z^2}$ solves the eqⁿ. $\left(\Rightarrow 2\frac{c}{z^3} = p\right)$

Using $\int_{z^*}^{\infty} p(z)\,dz = 1$ we obtain $c = (z^*)^2$

So far we have
$$\frac{1}{2}\int_{z^*}^{\infty} \frac{2(z^*)^2}{z^3}dz\Big([z,0] + [0,z]\Big) \to 1\,[z^*,z^*]$$
is transitively valid. But we must start with
$$\frac{1}{2}\Big([1,0] + [0,1]\Big).$$

Splitting imposes non-increasing average $\frac{1}{z}$.

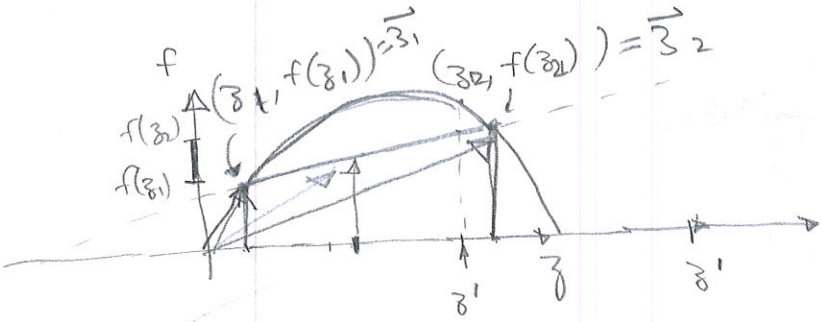
$$\Updownarrow$$

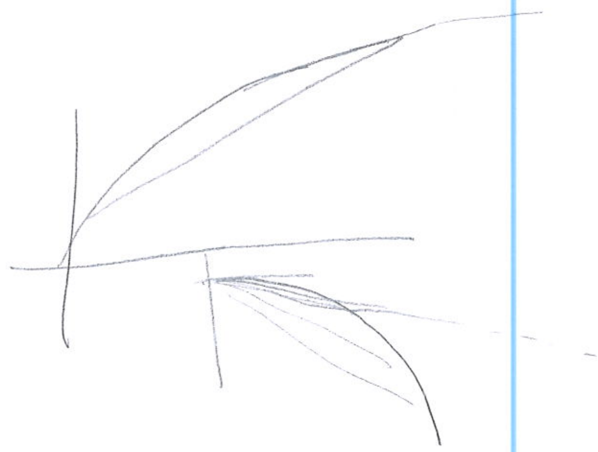
$$1 \geqslant \int_{z^*}^{\infty} \frac{p(z)}{z}dz = \int_{z^*}^{\infty} \frac{2(z^*)^2}{z^4}\,dz = \frac{2}{3z^*}$$

$$\Rightarrow \quad z^* \geqslant \frac{2}{3}.$$

$$\Rightarrow \quad \epsilon \geqslant 1/6.$$

—Rough—





$$\theta \, \vec{z}_2 + (1-\theta)\, \vec{z}_1$$

$$\theta z_2 + (1-\theta) z_1$$

$$\theta f(z_2) + (1-\theta) f(z_1) \leq f(\underbrace{\theta z_2 + (1-\theta) z_1})$$

monotone + concave