Certifying Local-Realism Violation

Manny

NIST

2014

Collaborators: K. Coakley, S. Glancy, S. W. Nam, Y. Zhang.

Overview

Test Configurations and Models

Bell Functions

Anti-Local-Realism Certificates

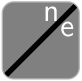
Applications to Experiments

Recommendations

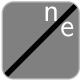
Parties, Settings and Measurements

- (2,2,2) (parties, settings choices, measurement outcomes):

A



A	00	01	10	11	B
n					n



B

Parties, Settings and Measurements

- (2,2,2) (parties, settings choices, measurement outcomes):

A

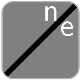
A	00	01	10	11	B
n	0	1	0	0	n

B

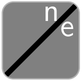
Parties, Settings and Measurements

- (2,2,2) (parties, settings choices, measurement outcomes):

A



A	00	01	10	11	B
n	0	1	0	0	n
n					e



B

Parties, Settings and Measurements

- (2,2,2) (parties, settings choices, measurement outcomes):

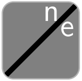
A

A	00	01	10	11	B
n	0	1	0	0	n
n	1	0	0	0	e

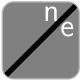
B

Parties, Settings and Measurements

- (2,2,2) (parties, settings choices, measurement outcomes):

A 

A	00	01	10	11	B
n	0	1	0	0	n
n	1	0	0	0	e
e					n



B

Parties, Settings and Measurements

- (2,2,2) (parties, settings choices, measurement outcomes):

A 

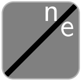
A	00	01	10	11	B
n	0	1	0	0	n
n	1	0	0	0	e
e	0	0	0	1	n

B

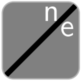
Parties, Settings and Measurements

- (2,2,2) (parties, settings choices, measurement outcomes):

A



A	00	01	10	11	B
n	0	1	0	0	n
n	1	0	0	0	e
e	0	0	0	1	n
e					e



B

Parties, Settings and Measurements

- (2,2,2) (parties, settings choices, measurement outcomes):

A 

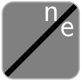
A	00	01	10	11	B
n	0	1	0	0	n
n	1	0	0	0	e
e	0	0	0	1	n
e	0	0	1	0	e

B

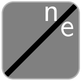
Parties, Settings and Measurements

- (2,2,2) (parties, settings choices, measurement outcomes):

A



A	00	01	10	11	B
n	0	1	0	0	n
n	1	0	0	0	e
e	0	0	0	1	n
e	0	0	1	0	e

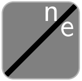


B

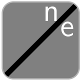
Parties, Settings and Measurements

- (2,2,2) (parties, settings choices, measurement outcomes):

A

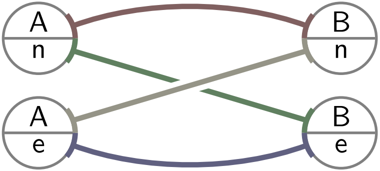


A	00	01	10	11	B
n	0	1	0	0	n
n	1	0	0	0	e
e	0	0	0	1	n
e	0	0	1	0	e



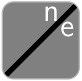
B

- Compatibility graph:

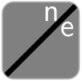


Parties, Settings and Measurements

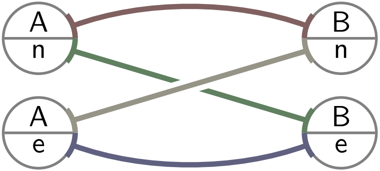
- (2,2,2) (parties, settings choices, measurement outcomes):

A 

A	00	01	10	11	B
n	0	1	0	0	n
n	1	0	0	0	e
e	0	0	0	1	n
e	0	0	1	0	e


B

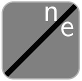
- Compatibility graph:



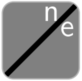
- *Trial* record: Outcomes and settings (o_A, o_B, s_A, s_B).

Parties, Settings and Measurements

- (2,2,2) (parties, settings choices, measurement outcomes):

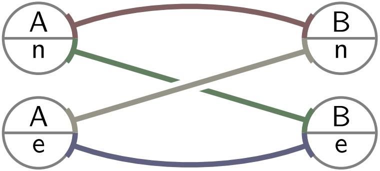
A 

A	00	01	10	11	B
n	0	1	0	0	n
n	1	0	0	0	e
e	0	0	0	1	n
e	0	0	1	0	e



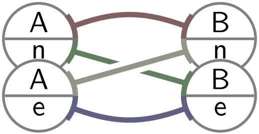
B

- Compatibility graph:

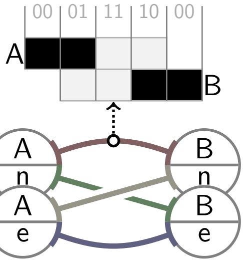


- *Trial* record: Outcomes and settings (o_A, o_B, s_A, s_B).
- Trial model: Prob$(O_A = o_A, O_B = o_B, S_A = s_B, S_B = s_B|\text{past})$.

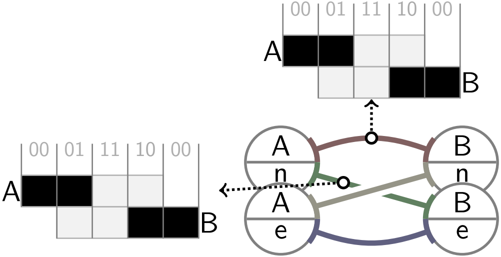
Example I



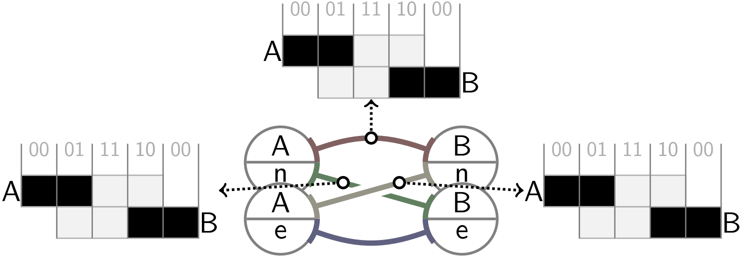
Example I



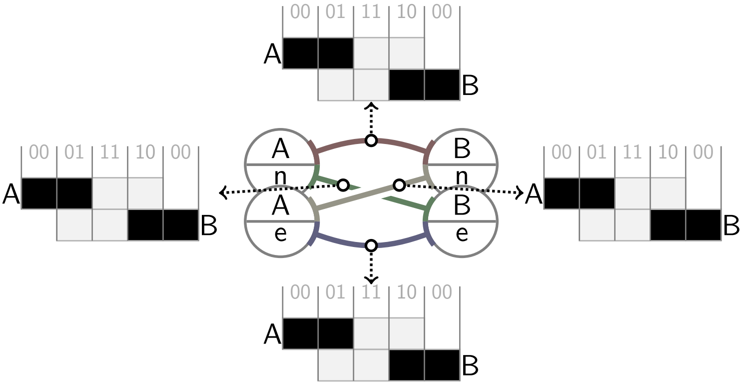
Example I



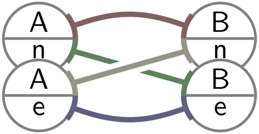
Example I



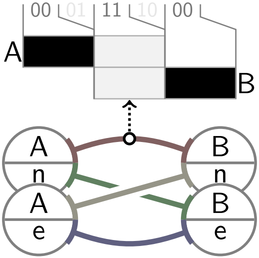
Example I


00 01 11 10 00
A
B
A
n
A
e
B
n
B
e
00 01 11 10 00
A
B
00 01 11 10 00
A
B
00 01 11 10 00
A
B

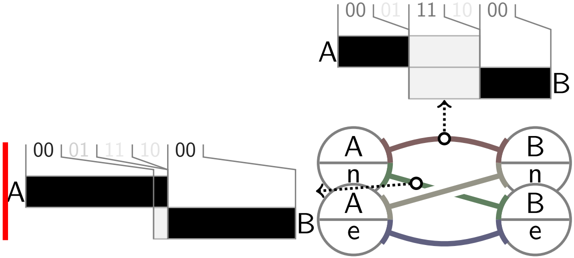
Examples II,III



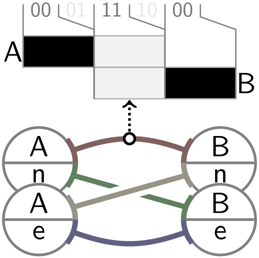
Examples II,III



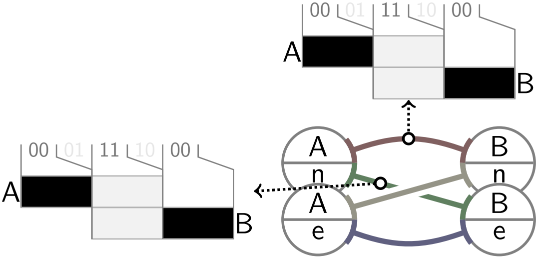
Examples II,III



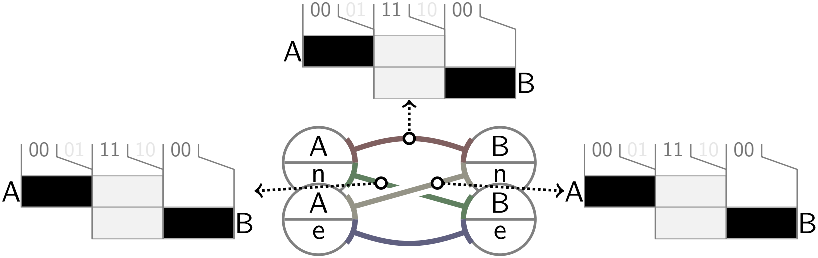
Examples II,III



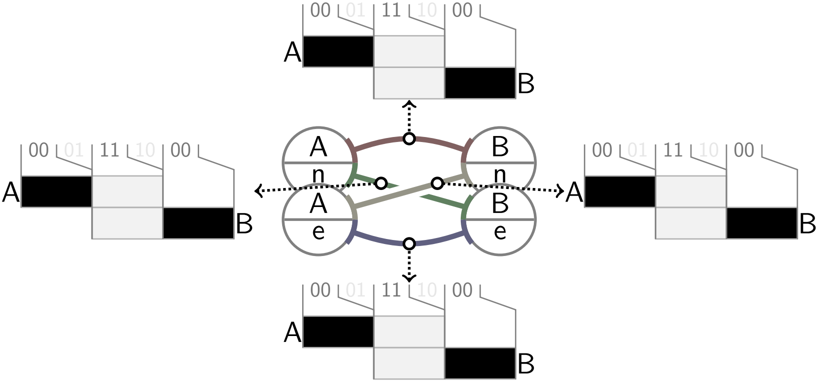
Examples II,III



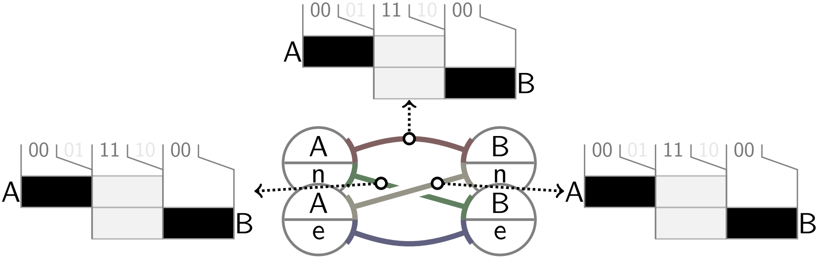
Examples II,III



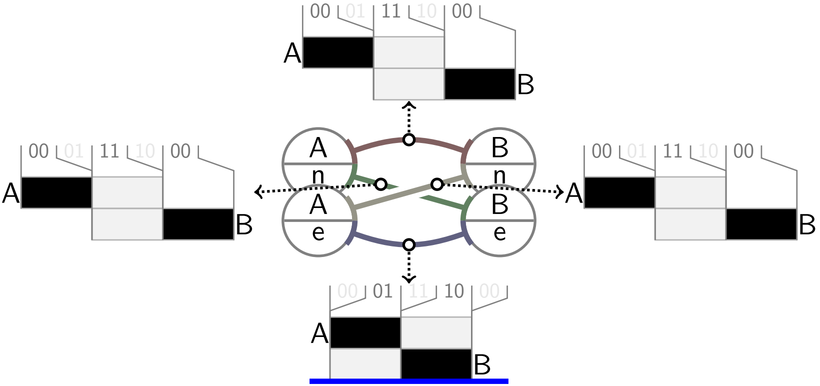
Examples II,III



Examples II,III

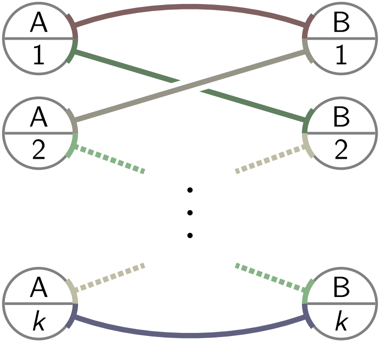


Examples II,III



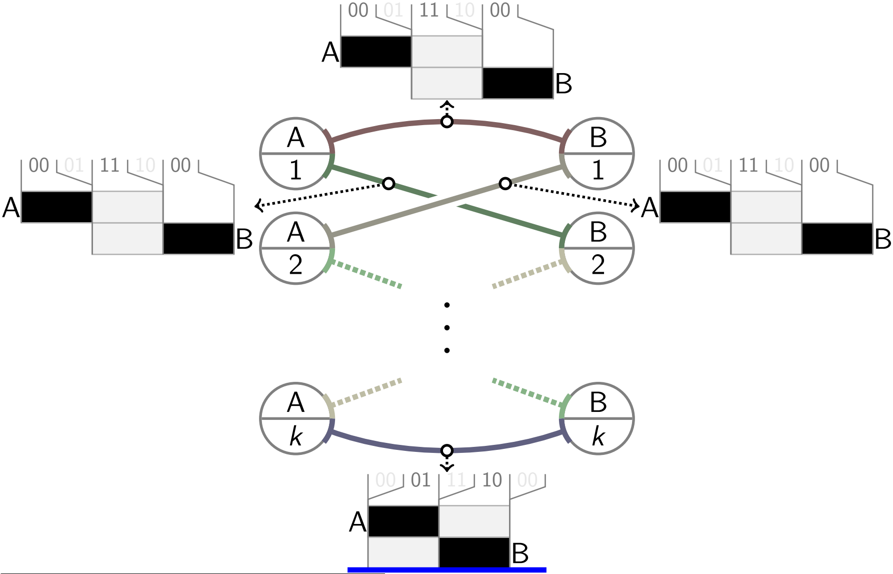
The PR Box, Popescu&Rohrlich(1997) [8].

The 2k-cycle



"chained Bell inequalities", Braunstein(1990) [1], application in Colbeck&Pironio(2011) [3]

The 2k-cycle



"chained Bell inequalities", Braunstein(1990) [1], application in Colbeck&Pironio(2011) [3]

General Measurement-Outcome Models

- One Trial:
  "Choose" measurement settings $\rightarrow$ measure $\rightarrow$ record outcomes.

General Measurement-Outcome Models

- One Trial:
  "Choose" measurement settings $\rightarrow$ measure $\rightarrow$ record outcomes.
- Common configuration parameters: (N_P, N_S, N_O), where

  N_P: Number of "parties".
  N_S: Number of measurement settings at each party.
  N_O: Number of possible outcomes for each setting.

General Measurement-Outcome Models

- One Trial:
  "Choose" measurement settings $\rightarrow$ measure $\rightarrow$ record outcomes.
- Common configuration parameters: (N_P, N_S, N_O), where

  N_P: Number of "parties".
  N_S: Number of measurement settings at each party.
  N_O: Number of possible outcomes for each setting.
- Universal pre-trial model.

  $S = (S_A, S_B, \ldots)$: settings random variables,
  $O = (O_A, O_B, \ldots)$: outcome random variables,

  with probability distribution:

$$\mu(o, s) = \mathrm{Prob}(O = o, S = s | \mathrm{past}).$$

General Measurement-Outcome Models

- One Trial:
  "Choose" measurement settings $\rightarrow$ measure $\rightarrow$ record outcomes.
- Common configuration parameters: (N_P, N_S, N_O), where

  N_P: Number of "parties".
  N_S: Number of measurement settings at each party.
  N_O: Number of possible outcomes for each setting.
- Universal pre-trial model.

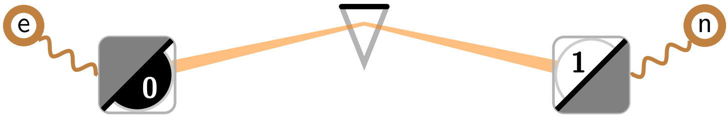
  $S = (S_A, S_B, \ldots)$: settings random variables,
  $O = (O_A, O_B, \ldots)$: outcome random variables,

  with probability distribution:

$$\mu(o, s) = \mathrm{Prob}(O = o, S = s|\mathrm{past}).$$

- Possible constraints:
  - Remote context independence/no-signaling/consistent marginals.
  - Remote outcome independence.
  - Definiteness given the "complete state".

Model Constraints to Consider

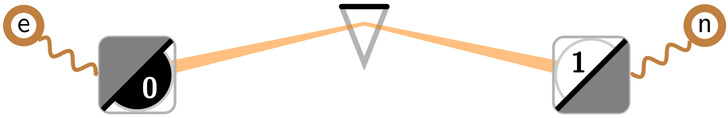


$s_A = \mathrm{e}$ $o_A = 0$ $o_B = 1$ $s_B = \mathrm{n}$

CI. Remote context independence.

$$\mu(o_X | s_X, s_{\neg X}) = \mu(o_X | s_X).$$

Model Constraints to Consider



$s_A = \mathsf{e}$ $o_A = 0$ $o_B = 1$ $s_B = \mathsf{n}$

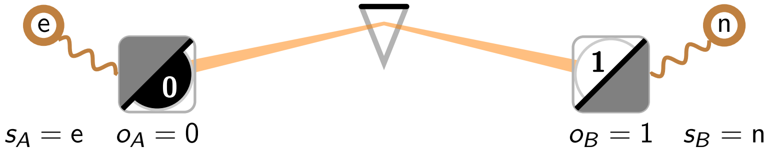
CI. Remote context independence.

$$\mu(o_X | s_X, s_{\neg X}) = \mu(o_X | s_X).$$

OI. Remote outcome independence.

$$\mu(o_X | o_{\neg X}, s) = \mu(o_X | s).$$

Model Constraints to Consider



CI. Remote context independence.

$$\mu(o_X | s_X, s_{\neg X}) = \mu(o_X | s_X).$$

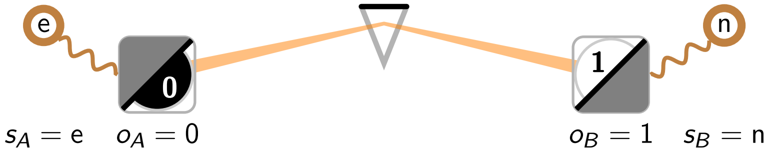
OI. Remote outcome independence.

$$\mu(o_X | o_{\neg X}, s) = \mu(o_X | s).$$

D. Definiteness given "complete state" f and settings.

$$o = (o_X)_X = (f_X(s))_X.$$

Model Constraints to Consider



CI. Remote context independence.

$$\mu(o_X | s_X, s_{\neg X}) = \mu(o_X | s_X).$$

OI. Remote outcome independence.

$$\mu(o_X | o_{\neg X}, s) = \mu(o_X | s).$$

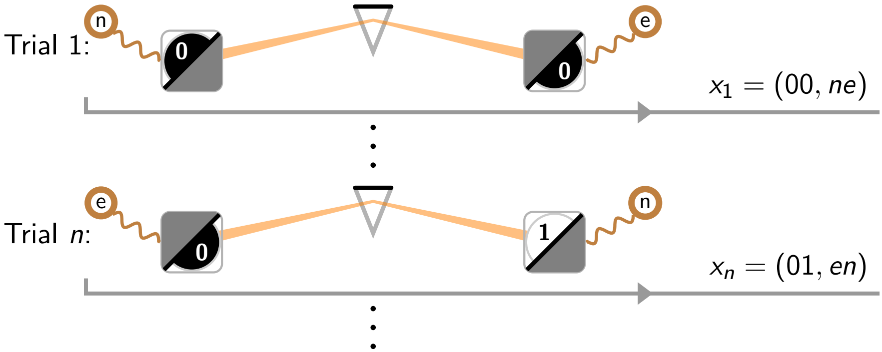
D. Definiteness given "complete state" f and settings.

$$o = (o_X)_X = (f_X(s))_X.$$

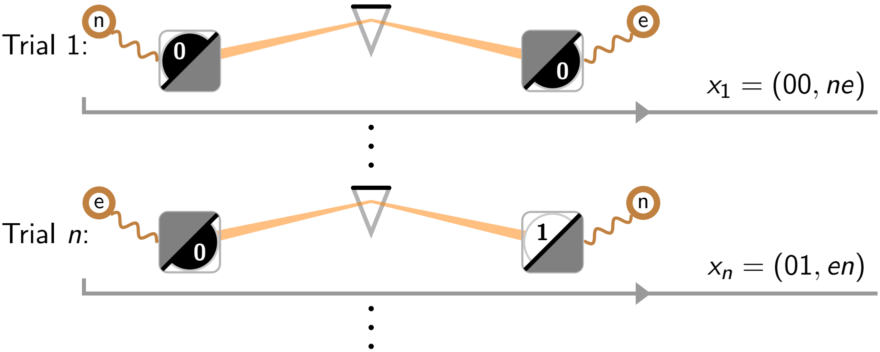
LR. Local realism, $\mathrm{CI} \wedge (\mathrm{OI} \vee \mathrm{D}) \wedge \mu(\lambda)$.

$$\mu(o, s) = \sum_{f:\text{for all } X \; f_X(s_x) = o_X} \mu(f)\mu(s).$$

Ideal Test



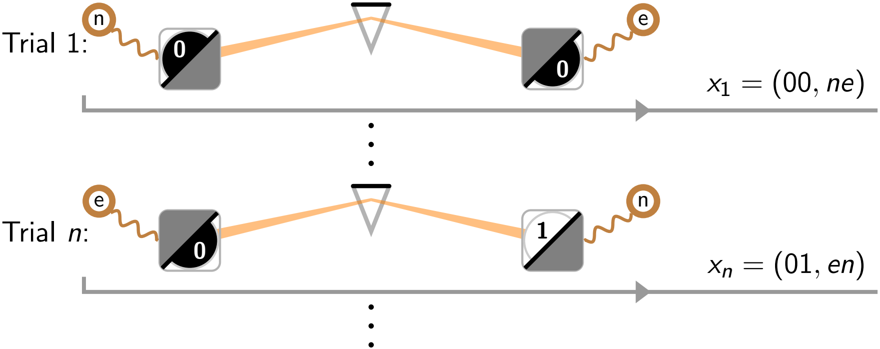
Ideal Test



From $\mathbf{x} = (x_1, \ldots, x_n, \ldots)$ compute $C_{\neg\mathcal{P}}(x)$, a certificate for $\neg\mathcal{P}$.

...where $\mathcal{P}$ is an "unwanted" property.

Ideal Test

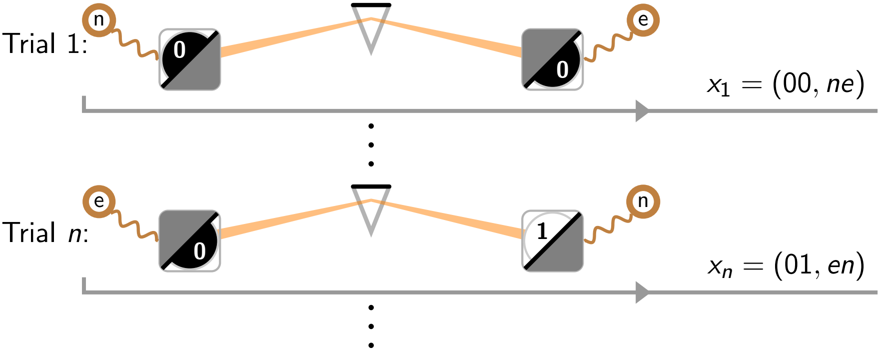


From $\mathbf{x} = (x_1, \ldots, x_n, \ldots)$ compute $C_{\neg\mathcal{P}}(x)$, a certificate for $\neg\mathcal{P}$.

...where $\mathcal{P}$ is an "unwanted" property.

- Foundations: Constrain explanatory models.

Ideal Test

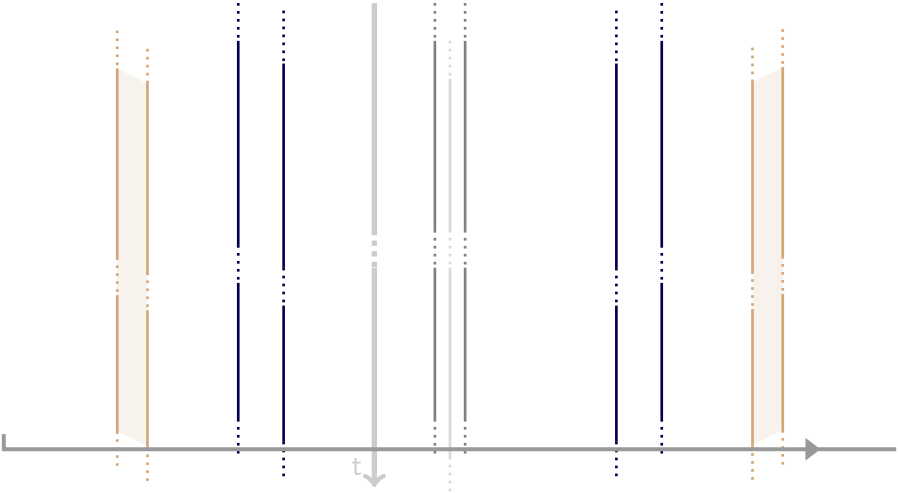


From $\mathbf{x} = (x_1, \ldots, x_n, \ldots)$ compute $C_{\neg\mathcal{P}}(x)$, a certificate for $\neg\mathcal{P}$.

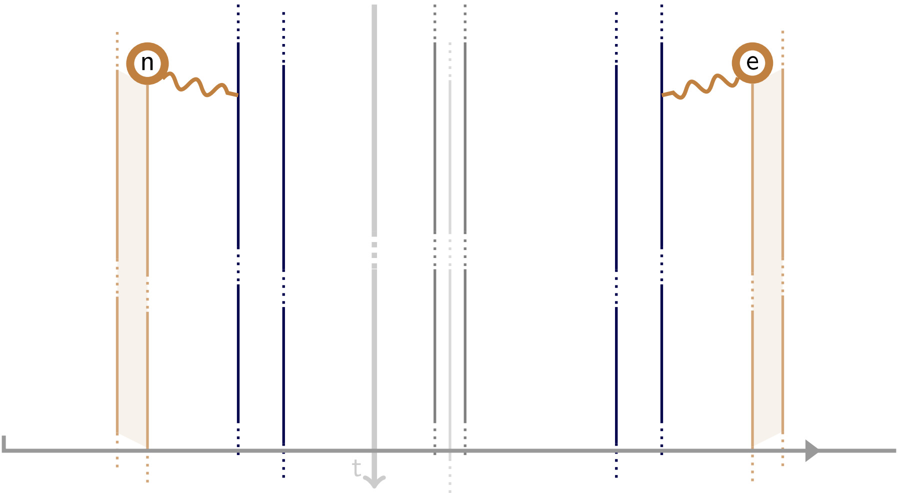
...where $\mathcal{P}$ is an "unwanted" property.

- Foundations: Constrain explanatory models.
- Protocols: Constrain hacker's access.

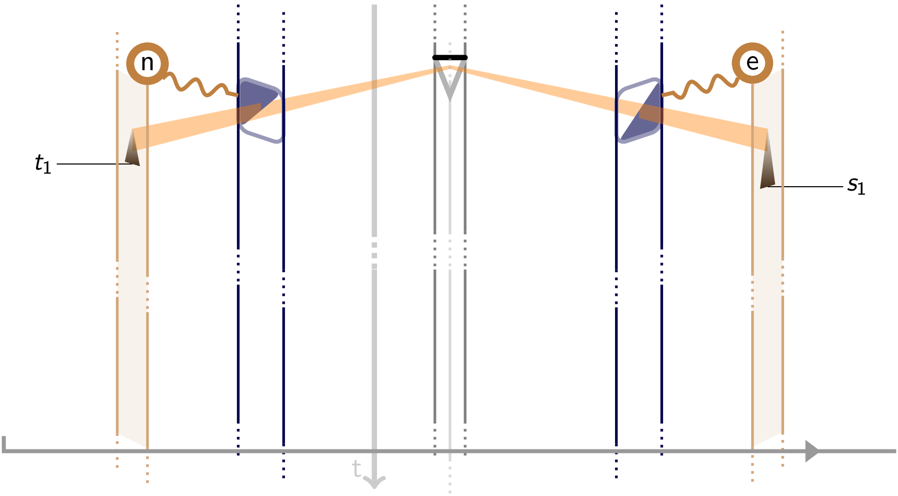
Common Photon-Based Trials



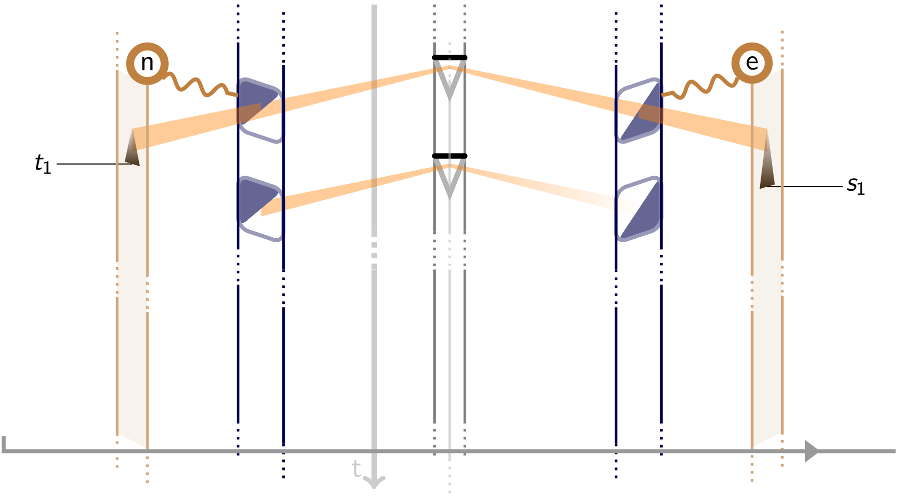
Common Photon-Based Trials



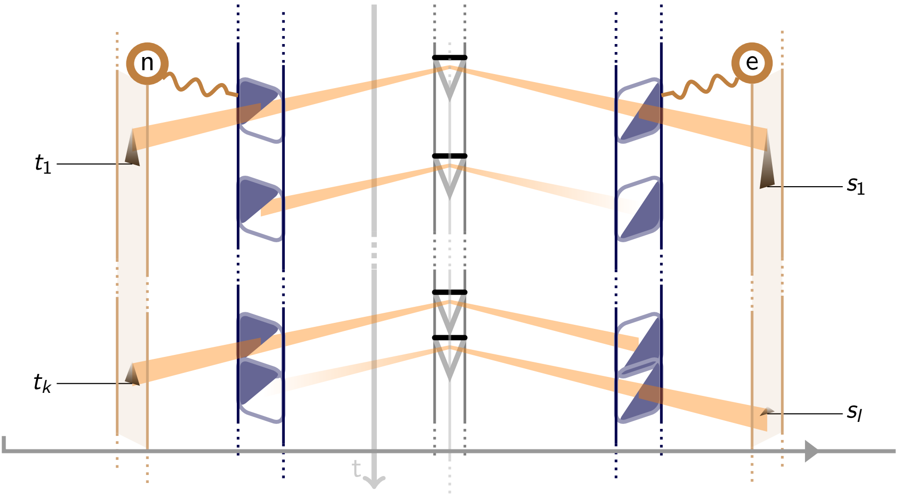
Common Photon-Based Trials



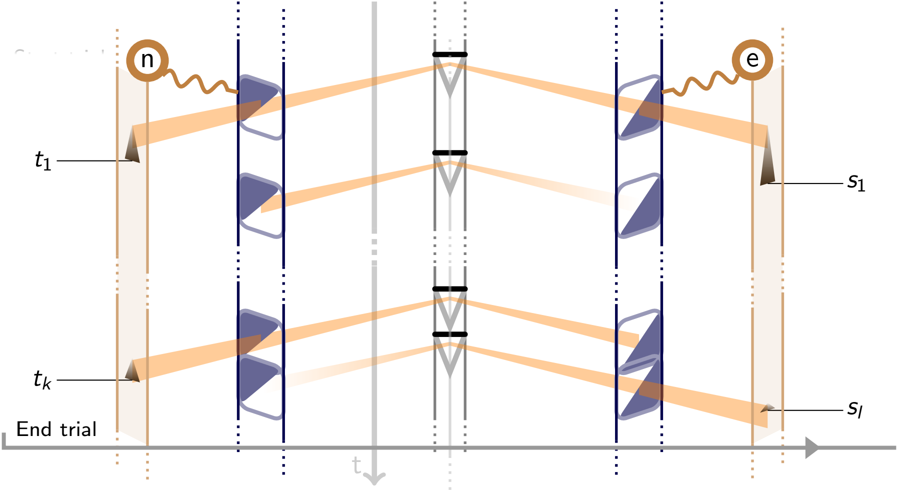
Common Photon-Based Trials



Common Photon-Based Trials



Common Photon-Based Trials



...this can be considered as *one* trial.

Recommendations

- Commit to deterministic trials. (W.o.l.g!)

Recommendations

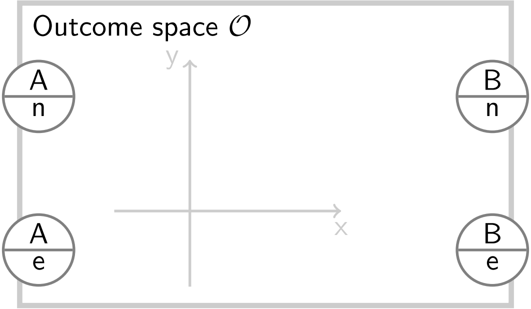
- Commit to deterministic trials. (W.o.l.g!)
- Change settings for each trial. (Make trials last longer if needed.)
- Any randomization helps avoid auxilliary assumptions.
- Blind the trials: Automated settings choices, no tweaking when settings are "visible".

Recommendations

- Commit to deterministic trials. (W.o.l.g!)
- Change settings for each trial. (Make trials last longer if needed.)
- Any randomization helps avoid auxilliary assumptions.
- Blind the trials: Automated settings choices, no tweaking when settings are "visible".
- Plan for generation of training data and confirmatory experiments.
- Compute certificates and gain rate per setting bit.
- Report: Certificate values, gain rates *and* model assumptions.

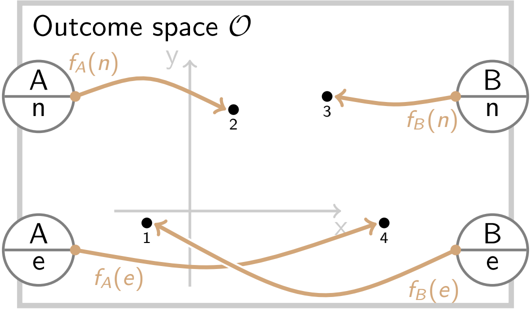
$(2, 2, \mathcal{O})$-Bell inequalities

LR:



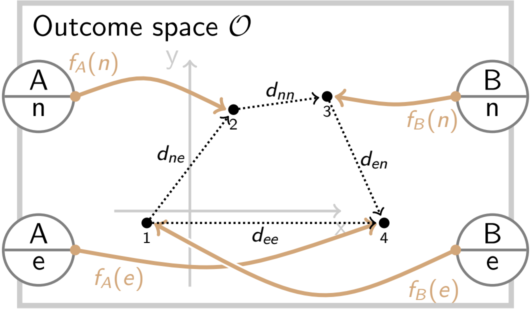
$(2, 2, \mathcal{O})$-Bell inequalities

LR:



$(2, 2, \mathcal{O})$-Bell inequalities

LR:

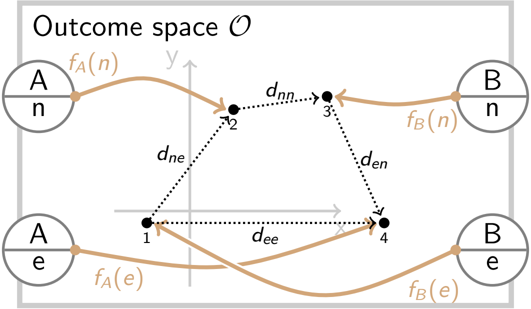


$$d_{ne} + d_{nn} + d_{en} \geq d_{ee} \quad \Rightarrow \quad \langle d_{ne} \rangle_\mu + \langle d_{nn} \rangle_\mu + \langle d_{en} \rangle_\mu \geq \langle d_{ee} \rangle_\mu$$

Timetag analysis (NIST 2013), Kurzynski&Kaszlikowski(2013) [6]

$(2, 2, \mathcal{O})$-Bell inequalities

LR:



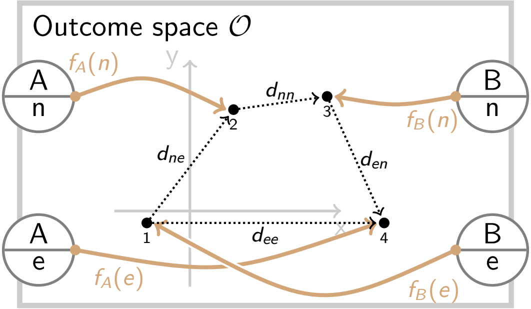
$$d_{ne} + d_{nn} + d_{en} \geq d_{ee} \quad \Rightarrow \quad \langle d_{ne}\rangle_\mu + \langle d_{nn}\rangle_\mu + \langle d_{en}\rangle_\mu \geq \langle d_{ee}\rangle_\mu$$

Settings independent of state $\Rightarrow$ $\langle d_{ab}\rangle = \langle d_{ab} | s = (a, b)\rangle.$

Timetag analysis (NIST 2013), Kurzynski&Kaszlikowski(2013) [6]

$(2, 2, \mathcal{O})$-Bell inequalities

LR:



$$d_{ne} + d_{nn} + d_{en} \geq d_{ee} \quad \Rightarrow \quad \langle d_{ne} \rangle_\mu + \langle d_{nn} \rangle_\mu + \langle d_{en} \rangle_\mu \geq \langle d_{ee} \rangle_\mu$$

Settings independent of state $\Rightarrow \quad \langle d_{ab} \rangle = \langle d_{ab} | s = (a, b) \rangle.$

Example. $\mathcal{O} = \{0, 1\}$: $\begin{cases} d(a,b) = |b - a| & \to \text{ CHSH variant,} \\ d(a,b) = \max(0, b - a) & \to \text{CH variant.} \end{cases}$

Timetag analysis (NIST 2013), Kurzynski&Kaszlikowski(2013) [6]

Bell Functions

Assumptions and context:

- RCI must hold for each trial. RCI:
  Remote context independence with control over settings dist. $p(s)$.

$$\mu(o_X|s) = \mu(o_X|s_X), \qquad \mu(o, s) = \mu(o|s)p(s).$$

Bell Functions

Assumptions and context:

- RCI must hold for each trial. RCI:
  Remote context independence with control over settings dist. $p(s)$.

$$\mu(o_X|s) = \mu(o_X|s_X), \qquad \mu(o,s) = \mu(o|s)p(s).$$

- If LRI, then abandon ship. LRI:
  LR with independent full-support settings distribution.

$$\mu(o,s) = \mu(f : \text{for all } X, f_{X,s_x} = o_x)p(s), \qquad p(s) > 0.$$

Bell Functions

Assumptions and context:

- RCI must hold for each trial. RCI:
  Remote context independence with control over settings dist. $p(s)$.

$$\mu(o_X|s) = \mu(o_X|s_X), \qquad \mu(o, s) = \mu(o|s)p(s).$$

- If LRI, then abandon ship. LRI:
  LR with independent full-support settings distribution.

$$\mu(o, s) = \mu(f : \text{for all } X, f_{X,s_x} = o_x)p(s), \qquad p(s) > 0.$$

- If not LRI, invoke loopholes or bug?

Bell Functions

Assumptions and context:

- RCI must hold for each trial. RCI:
  Remote context independence with control over settings dist. $p(s)$.

$$\mu(o_X|s) = \mu(o_X|s_X), \qquad \mu(o,s) = \mu(o|s)p(s).$$

- If LRI, then abandon ship. LRI:
  LR with independent full-support settings distribution.

$$\mu(o,s) = \mu(f : \text{for all } X, f_{X,s_x} = o_x)p(s), \qquad p(s) > 0.$$

- If not LRI, invoke loopholes or bug?

Bell function: A function $B : (o,s) \mapsto B(o,s) \in \mathbb{R}$ satisfying

$$b_{B,p} \doteq \sup_{\mu \in \mathrm{LRI}(p)} \langle B(O,S) \rangle_\mu \quad < \quad \sup_{\mu \in \mathrm{RCI}(p)} \langle B(O,S) \rangle_\mu$$

Measuring Bell-Functions

Given: Trial results $(o_1, s_1), \ldots, (o_N, s_N)$.

Measuring Bell-Functions

Given: Trial results $(o_1, s_1), \ldots, (o_N, s_N)$.

Optimistic assumption: Every trial is independent and identical.

Measuring Bell-Functions

Given: Trial results $(o_1, s_1), \ldots, (o_N, s_N)$.

Optimistic assumption: Every trial is independent and identical.
Tradition: Empirically estimate $\langle B(O, S)\rangle$:

1. Compute the sample mean $\bar{b} = \sum_i B(o_i, s_i)/N$.
2. Compute the sample variance s^2.
3. Report $B = \bar{b} \pm s$ and *nominal SNR* $s/(\bar{b} - b_{B,p})$.

Measuring Bell-Functions

Given: Trial results $(o_1, s_1), \ldots, (o_N, s_N)$.

Optimistic assumption: Every trial is independent and identical.
Tradition: Empirically estimate $\langle B(O, S)\rangle$:

1. Compute the sample mean $\bar{b} = \sum_i B(o_i, s_i)/N$.
2. Compute the sample variance s^2.
3. Report $B = \bar{b} \pm s$ and *nominal SNR* $s/(\bar{b} - b_{B,p})$.

Conservative assumption: Trials depend on history, states vary.

Measuring Bell-Functions

Given: Trial results $(o_1, s_1), \ldots, (o_N, s_N)$.

Optimistic assumption: Every trial is independent and identical.
Tradition: Empirically estimate $\langle B(O, S)\rangle$:

1. Compute the sample mean $\bar{b} = \sum_i B(o_i, s_i)/N$.
2. Compute the sample variance s^2.
3. Report $B = \bar{b} \pm s$ and *nominal SNR* $s/(\bar{b} - b_{B,p})$.

Conservative assumption: Trials depend on history, states vary.
Emulate tradition: Empirically estimate $\sum_i \langle B(O_i, S_i)|\text{past}_i\rangle/N$:

1. Compute the sample mean $\bar{b} = \sum_i B(o_i, s_i)/N$.
2. Empirically upper bound the "martingale variance" s^2.
3. Report $B = \bar{b} \pm s$ and *nominal SNR* $s/(\bar{b} - b_{B,p})$.

Measuring Bell-Functions

Given: Trial results $(o_1, s_1), \ldots, (o_N, s_N)$.

Optimistic assumption: Every trial is independent and identical.
Tradition: Empirically estimate $\langle B(O, S)\rangle$:

1. Compute the sample mean $\bar{b} = \sum_i B(o_i, s_i)/N$.
2. Compute the sample variance s^2.
3. Report $B = \bar{b} \pm s$ and *nominal SNR* $s/(\bar{b} - b_{B,p})$.

Conservative assumption: Trials depend on history, states vary.
Emulate tradition: Empirically estimate $\sum_i \langle B(O_i, S_i)|\text{past}_i\rangle/N$:

1. Compute the sample mean $\bar{b} = \sum_i B(o_i, s_i)/N$.
2. Empirically upper bound the "martingale variance" s^2.
3. Report $B = \bar{b} \pm s$ and *nominal SNR* $s/(\bar{b} - b_{B,p})$.

Interpretation:
Average Bell-values of trial states with confidence intervals.

Interpreting Bell Values

Given: Trial results $(o_1, s_1), \ldots, (o_N, s_N)$.

$\vdots$

3. Report $B = \bar{b} \pm s$ and *nominal SNR* $s/(\bar{b} - b_{B,p})$.

Interpreting Bell Values

Given: Trial results $(o_1, s_1), \ldots, (o_N, s_N)$.

$\vdots$

3. Report $B = \bar{b} \pm s$ and *nominal SNR* $s/(\bar{b} - b_{B,p})$.

Specific to this experimental run:

- $b \in [\bar{b} - s, \bar{b} + s]$ at confidence level 68 %.
- Nominal SNR: Qualitative strength of exceeding LRI bound.

. . . central limit theorem does not apply.

Interpreting Bell Values

Given: Trial results $(o_1, s_1), \ldots, (o_N, s_N)$.

⋮

3. Report $B = \bar{b} \pm s$ and *nominal SNR* $s/(\bar{b} - b_{B,p})$.

Specific to this experimental run:

- $b \in [\bar{b} - s, \bar{b} + s]$ at confidence level 68 %.
- Nominal SNR: Qualitative strength of exceeding LRI bound.

. . . central limit theorem does not apply.

Comparative:

- Different runs of the same experiment.
- Results from different experiments w. identical config., state.

Interpreting Bell Values

Given: Trial results $(o_1, s_1), \ldots, (o_N, s_N)$.

$\vdots$

3. Report $B = \bar{b} \pm s$ and *nominal SNR* $s/(\bar{b} - b_{B,p})$.

Specific to this experimental run:

- $b \in [\bar{b} - s, \bar{b} + s]$ at confidence level 68 %.
- Nominal SNR: Qualitative strength of exceeding LRI bound.

. . . central limit theorem does not apply.

Comparative:

- Different runs of the same experiment.
- Results from different experiments w. identical config., state.

Not addressed:

- Fair comparison of experiments w. different configurations, Bell functions, assumptions.
- Fair comparison of implemented trials.
- Quantify ability of LRI to yield observed effects.

Anti-LRI Certificates

Context:	Expect non-LRI signature in the absence of a conspiracy, but quantified reassurance needed.
Bonus:	Solve issues with nominal SNRs.

Anti-LRI Certificates

Context:	Expect non-LRI signature in the absence of a conspiracy, but quantified reassurance needed.
Bonus:	Solve issues with nominal SNRs.

Solution: Construct and use positive, mean ≤ 1 Bell functions.

1. Choose Bell fn. $B(O,S)$ with $B(O,S) \geq l_B$, $\langle B(O,S)\rangle_{\mathrm{LRI},p} \leq b_{B,p}$.

Y. Zhang et al. (2013) [13], General theory: Shafer et al. (2011) [9]

Anti-LRI Certificates

Context:	Expect non-LRI signature in the absence of a conspiracy, but quantified reassurance needed.
Bonus:	Solve issues with nominal SNRs.

Solution: Construct and use positive, mean ≤ 1 Bell functions.

1. Choose Bell fn. $B(O,S)$ with $B(O,S) \geq l_B$, $\langle B(O,S)\rangle_{\mathrm{LRI},p} \leq b_{B,p}$.
2. Shift and scale $P(O,S) \doteq (B(O,S) - l_B)/(b_{B,p} - l_B)$ so $P(O,S) \geq 0$, $\langle P(O,S)\rangle_{\mathrm{LRI},p} \leq 1$, and hence

$$\left\langle S_N \doteq \prod_{i=1}^{N} P(O_i, S_i|\mathrm{past}_i) \right\rangle_{\mathrm{LRI},p} \leq 1.$$

Y. Zhang et al. (2013) [13], General theory: Shafer et al. (2011) [9]

Anti-LRI Certificates

Context:	Expect non-LRI signature in the absence of a conspiracy, but quantified reassurance needed.
Bonus:	Solve issues with nominal SNRs.

Solution: Construct and use positive, mean ≤ 1 Bell functions.

1. Choose Bell fn. $B(O,S)$ with $B(O,S) \geq l_B$, $\langle B(O,S)\rangle_{\mathrm{LRI},p} \leq b_{B,p}$.
2. Shift and scale $P(O,S) \doteq (B(O,S) - l_B)/(b_{B,p} - l_B)$ so $P(O,S) \geq 0$, $\langle P(O,S)\rangle_{\mathrm{LRI},p} \leq 1$, and hence

$$\left\langle S_N \doteq \prod_{i=1}^{N} P(O_i, S_i|\mathrm{past}_i) \right\rangle_{\mathrm{LRI},p} \leq 1.$$

3. Get trial data $\ldots(o_i, s_i)\ldots$, compute s_N, note:

$$\mathrm{Prob}(S_N \geq s_N|\mathrm{LRI}, p) \leq 1/s_N. \qquad \text{(Markov's inequality)}$$

Y. Zhang et al. (2013) [13], General theory: Shafer et al. (2011) [9]

Anti-LRI Certificates

Context:	Expect non-LRI signature in the absence of a conspiracy, but quantified reassurance needed.
Bonus:	Solve issues with nominal SNRs.

Solution: Construct and use positive, mean ≤ 1 Bell functions.

1. Choose Bell fn. $B(O,S)$ with $B(O,S) \geq l_B$, $\langle B(O,S)\rangle_{\mathrm{LRI},p} \leq b_{B,p}$.
2. Shift and scale $P(O,S) \doteq (B(O,S) - l_B)/(b_{B,p} - l_B)$ so $P(O,S) \geq 0$, $\langle P(O,S)\rangle_{\mathrm{LRI},p} \leq 1$, and hence

$$\left\langle S_N \doteq \prod_{i=1}^{N} P(O_i, S_i|\mathrm{past}_i)\right\rangle_{\mathrm{LRI},p} \leq 1.$$

3. Get trial data $\ldots(o_i, s_i)\ldots$, compute s_N, note:

$$\mathrm{Prob}(S_N \geq s_N|\mathrm{LRI}, p) \leq 1/s_N. \qquad \text{(Markov's inequality)}$$

4. Cert. $c \doteq \log_2(s_N)$, gain-rate/trial/set.-bit $g \doteq \log_2(s_N)/(H(p)N)$.

Y. Zhang et al. (2013) [13], General theory: Shafer et al. (2011) [9]

Interpretation of Anti-LRI Certificates

$$P(O,S) \geq 0,\ \langle P(O,S)\rangle_{\mathrm{LRI},p} \leq 1,\ \left\langle S_N \doteq \prod_{i=1}^{N} P(O_i,S_i|\mathrm{past}_i)\right\rangle_{\mathrm{LRI},p} \leq 1.$$

⋮

$$\mathrm{Prob}(S_N \geq s_N|\mathrm{LRI},p) \leq 1/s_N.$$

4. Cert. $c \doteq \log_2(s_N)$, gain-rate/trial/set.-bit $g \doteq \log_2(s_N)/(H(p)N)$.

Antecedents: Gill (2003) [4], van Dam et al. (2005) [10]

Interpretation of Anti-LRI Certificates

$P(O,S) \geq 0$, $\langle P(O,S)\rangle_{\text{LRI},p} \leq 1$, $\left\langle S_N \doteq \prod_{i=1}^{N} P(O_i, S_i|\text{past}_i)\right\rangle_{\text{LRI},p} \leq 1.$

⋮

$$\text{Prob}(S_N \geq s_N|\text{LRI}, p) \leq 1/s_N.$$

4. Cert. $c \doteq \log_2(s_N)$, gain-rate/trial/set.-bit $g \doteq \log_2(s_N)/(H(p)N)$.

Statistical:

- $\text{LRI}(p) \Rightarrow$ prob. of certifying at $\geq c$ is less then 2^{-c}.
- Equivalent to a p-value bound...
- Bayes-factor-like. E.g. stop any time.

Antecedents: Gill (2003) [4], van Dam et al. (2005) [10]

Interpretation of Anti-LRI Certificates

$$P(O,S) \geq 0,\ \langle P(O,S)\rangle_{\mathrm{LRI},p} \leq 1,\ \left\langle S_N \doteq \prod_{i=1}^{N} P(O_i, S_i|\mathrm{past}_i)\right\rangle_{\mathrm{LRI},p} \leq 1.$$

$\vdots$

$$\mathrm{Prob}(S_N \geq s_N|\mathrm{LRI}, p) \leq 1/s_N.$$

4. Cert. $c \doteq \log_2(s_N)$, gain-rate/trial/set.-bit $g \doteq \log_2(s_N)/(H(p)N)$.

Statistical:

- LRI(p) $\Rightarrow$ prob. of certifying at $\geq c$ is less then 2^{-c}.
- Equivalent to a p-value bound...
- Bayes-factor-like. E.g. stop any time.

Comparative:

- Certificate: Comparable overall strength.
- Gain rate: Comparable device/configuration strength.
- Independent of experimental details or Bell function, given model assumptions.

Antecedents: Gill (2003) [4], van Dam et al. (2005) [10]

Recent Experiments

- Pironio et al. (2010) [7]:
  - Entangled atoms in two iontraps at 1 m.
  - Aim: Certified random number expansion.
  - Average CHSH value: $2 < 2.41(6)$ per trial for 3016 trials. Nominal SNR: 6.8.
  - Certificate ($\log_2$-p): 10 [7], $33 \equiv 6.3$ g.SNR [12, 11].

Recent Experiments

- Pironio et al. (2010) [7]:
  - Entangled atoms in two iontraps at 1 m.
  - Aim: Certified random number expansion.
  - Average CHSH value: $2 < 2.41(6)$ per trial for 3016 trials. Nominal SNR: 6.8.
  - Certificate ($\log_2$-p): 10 [7], $33 \equiv 6.3$ g.SNR [12, 11].
- Giustina et al. (2013) [5]:
  - Entangled photons, continuously emitted, timetagged detections.
  - Aim: Bell violation without postselection.
  - Average Bell function value: $0 < 5.24(8)10^{-3}$ per photon-pair [5]. Nominal SNR: 66.
  - Timetag function value: $1.083(19 \mid 35)10^5$, nominal SNR 59 or 31.
  - Justify coverage probability, certificate?

Recent Experiments

- Pironio et al. (2010) [7]:
  - Entangled atoms in two iontraps at 1 m.
  - Aim: Certified random number expansion.
  - Average CHSH value: $2 < 2.41(6)$ per trial for 3016 trials. Nominal SNR: 6.8.
  - Certificate ($\log_2$-p): 10 [7], $33 \equiv 6.3$ g.SNR [12, 11].
- Giustina et al. (2013) [5]:
  - Entangled photons, continuously emitted, timetagged detections.
  - Aim: Bell violation without postselection.
  - Average Bell function value: $0 < 5.24(8)10^{-3}$ per photon-pair [5]. Nominal SNR: 66.
  - Timetag function value: $1.083(19 \mid 35)10^{5}$, nominal SNR 59 or 31.
  - Justify coverage probability, certificate?
- Christensen et al. (2013) [2]:
  - Entangled photons, pulsed emission, timetagged detections.
  - Aim: Bell violation without postselection.
  - Average Bell function value: $0 < 5.4(7)10^{-5}$ per trial, n.SNR 7.7.
  - PBR certificate ($\log_2$-p): TBD

Recommendations

- Commit to deterministic trials. (W.o.l.g!)

Recommendations

- Commit to deterministic trials. (W.o.l.g!)
- Change settings for each trial. (Make trials last longer if needed.)
- Any randomization helps avoid auxilliary assumptions.
- Blind the trials: Automated settings choices, no tweaking when settings are “visible”.

Recommendations

- Commit to deterministic trials. (W.o.l.g!)
- Change settings for each trial. (Make trials last longer if needed.)
- Any randomization helps avoid auxilliary assumptions.
- Blind the trials: Automated settings choices, no tweaking when settings are "visible".
- Plan for generation of training data and confirmatory experiments.
- Compute certificates and gain rate per setting bit.
- Report: Certificate values, gain rates *and* model assumptions.

PBRs: Optimizing Certificate Algorithms

$$P(O,S) \geq 0,\ \langle P(O,S)\rangle_{\mathrm{LRI},p} \leq 1,\ \left\langle S_N \doteq \prod_{i=1}^{N} P(O_i, S_i|\mathrm{past}_i)\right\rangle_{\mathrm{LRI},p} \leq 1.$$

$\vdots$

$$\mathrm{Prob}(S_N \geq s_N|\mathrm{LRI}, p) \leq 1/s_N.$$

4. Cert. $c \doteq \log_2(s_N)$, gain-rate/trial/set.-bit $g \doteq \log_2(s_N)/(H(p)N)$.

PBRs: Optimizing Certificate Algorithms

$P(O,S) \geq 0$, $\langle P(O,S)\rangle_{\mathrm{LRI},p} \leq 1$, $\left\langle S_N \doteq \prod_{i=1}^{N} P(O_i, S_i|\mathrm{past}_i)\right\rangle_{\mathrm{LRI},p} \leq 1.$

⋮

$$\mathrm{Prob}(S_N \geq s_N|\mathrm{LRI}, p) \leq 1/s_N.$$

4. Cert. $c \doteq \log_2(s_N)$, gain-rate/trial/set.-bit $g \doteq \log_2(s_N)/(H(p)N)$.

Flexible function choice:

- Optimize convex combination of PBR functions.
  (Use theory or training set.) PBR: Probability Based Ratio.
- LRI tests: Include “trivial” and no-signalling constraints.

PBRs: Optimizing Certificate Algorithms

$P(O,S) \geq 0$, $\langle P(O,S)\rangle_{\mathrm{LRI},p} \leq 1$, $\left\langle S_N \doteq \prod_{i=1}^{N} P(O_i, S_i|\mathrm{past}_i)\right\rangle_{\mathrm{LRI},p} \leq 1$.

$\vdots$

$$\mathrm{Prob}(S_N \geq s_N|\mathrm{LRI}, p) \leq 1/s_N.$$

4. Cert. $c \doteq \log_2(s_N)$, gain-rate/trial/set.-bit $g \doteq \log_2(s_N)/(H(p)N)$.

Flexible function choice:

- Optimize convex combination of PBR functions.
  (Use theory or training set.)

PBR: Probability Based Ratio.

- LRI tests: Include "trivial" and no-signalling constraints.

Adaptive PBR functions:

- $P \to P_i$, chosen optimally before i'th trial.

PBRs: Optimizing Certificate Algorithms

$P(O,S) \geq 0$, $\langle P(O,S)\rangle_{\mathrm{LRI},p} \leq 1$, $\left\langle S_N \doteq \prod_{i=1}^{N} P(O_i, S_i|\mathrm{past}_i)\right\rangle_{\mathrm{LRI},p} \leq 1$.

⋮

$$\mathrm{Prob}(S_N \geq s_N|\mathrm{LRI}, p) \leq 1/s_N.$$

4. Cert. $c \doteq \log_2(s_N)$, gain-rate/trial/set.-bit $g \doteq \log_2(s_N)/(H(p)N)$.

Flexible function choice:

- Optimize convex combination of PBR functions.
  (Use theory or training set.)

PBR: Probability Based Ratio.

- LRI tests: Include "trivial" and no-signalling constraints.

Adaptive PBR functions:

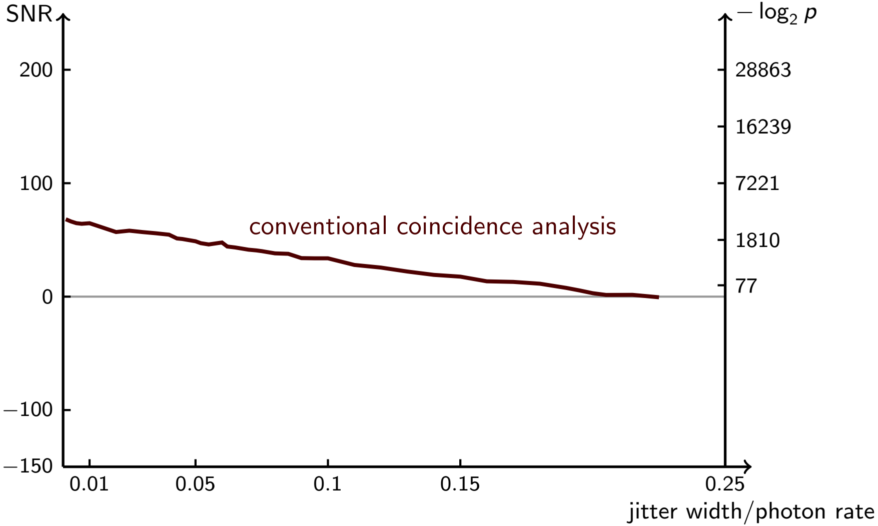
- $P \to P_i$, chosen optimally before i'th trial.

Features:

- Adapts to changing states, experimental drifts; stop anytime.
- Matches or improves other approaches (e.g. Hoeffding bounds).
- Asymptotically optimal when trials are i.i.d.
- Can automatically optimize equivalent Gaussian SNR.
- Adaptable to unbounded triangle-inequality Bell functions.

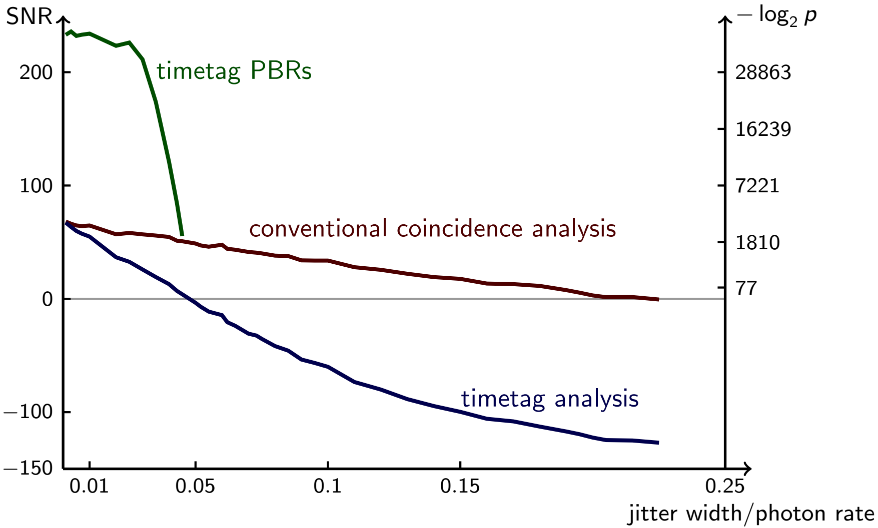
Simulation: Quantum Timetag Trials

Specs: Poisson pairs, efficiency 80 %, square jitter.
1 detector/party, CHSH optimized.



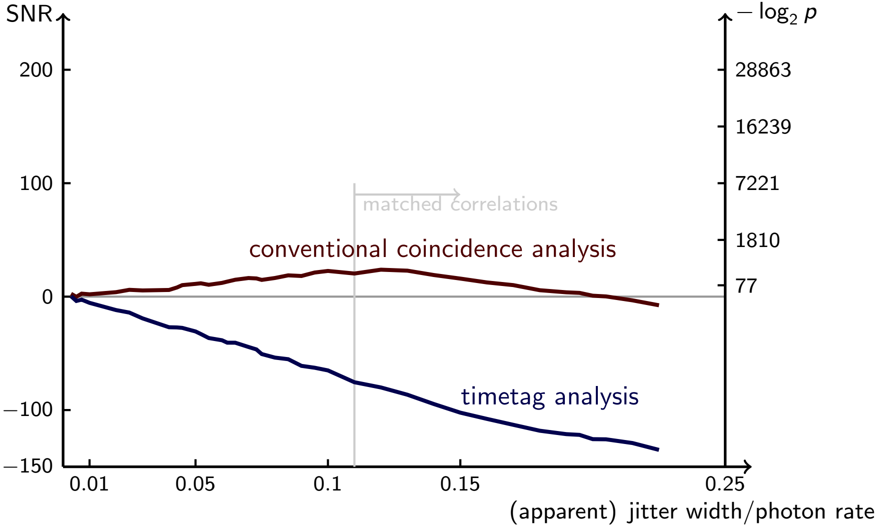
Simulation: Quantum Timetag Trials

Specs: Poisson pairs, efficiency 80 %, square jitter.
1 detector/party, CHSH optimized.



Simulation: LRI Timetag Trials

Specs: Match 1st and 2nd-order q. counting statistics at high apparent jitter.



TOC I

References I

[1] S. L. Braunstein. Wringing out better Bell inequalities. *Ann. der Physik*, 202:22–56, 1990.

[2] B. G. Christensen, K. T. McCusker, J. Altepeter, B. Calkins, T. Gerrits, A. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam Nd N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat. Detection-loophole-free test of quantum nonlocality, and applications. *Phys. Rev. Lett.*, 111:130406/1–5, 2013.

[3] R. Colbeck and R. Reneer. Free randomness can be amplifed. *Nature Phys.*, 8:450–453, 2012. arXiv:1105.3195.

[4] R. D. Gill. Time, finite statistics, and Bell's fifth position. arXiv:quant-ph/0301059, 2003.

[5] M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, R. Ursin, and A. Zeilinger. Bell violation using entangled photons without the fair-sampling assumptions. *Nature*, 2013.

[6] P. Kurzynski and D. Kaszlikowski. The triangle principle: A new approach to non-contextuality and local realism. arXiv:1309.6777, 2013.

[7] S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by bell's theorem. *Nature*, 464:1021–1024, 2010.

[8] S. Popescu and D. Rohrlich. Causality and nonlocality as axioms for quantum mechanics. *Found. Phys.*, 24:379–385, 1997.

[9] G. Shafer, A. Shen, N. Vereshchagin, and V. Vovk. Test martingales, Bayes factors and p-values. *Statistical Science*, 26:84–101, 2011.

[10] W. van Dam, R. D. Gill, and P. D. Grunwald. The statistical strength of nonlocality proofs. *IEEE Trans. Inf. Theory*, 51:2812–2835, 2005.

[11] Y. Zhang. *Analysis of Tests of Local Realism*. PhD thesis, U. Colorado at Boulder, Boulder, CO, 2013.

[12] Y. Zhang, S. Glancy, and E. Knill. Asymptotically optimal data analysis for rejecting local realism. *Phys. Rev. A*, 84:062118/1–10, 2011.

References II

[13] Y. Zhang, S. Glancy, and E. Knill. Efficient quantification of experimental evidence against local realism. *Phys. Rev. A*, 88:052119/1–8, 2013.