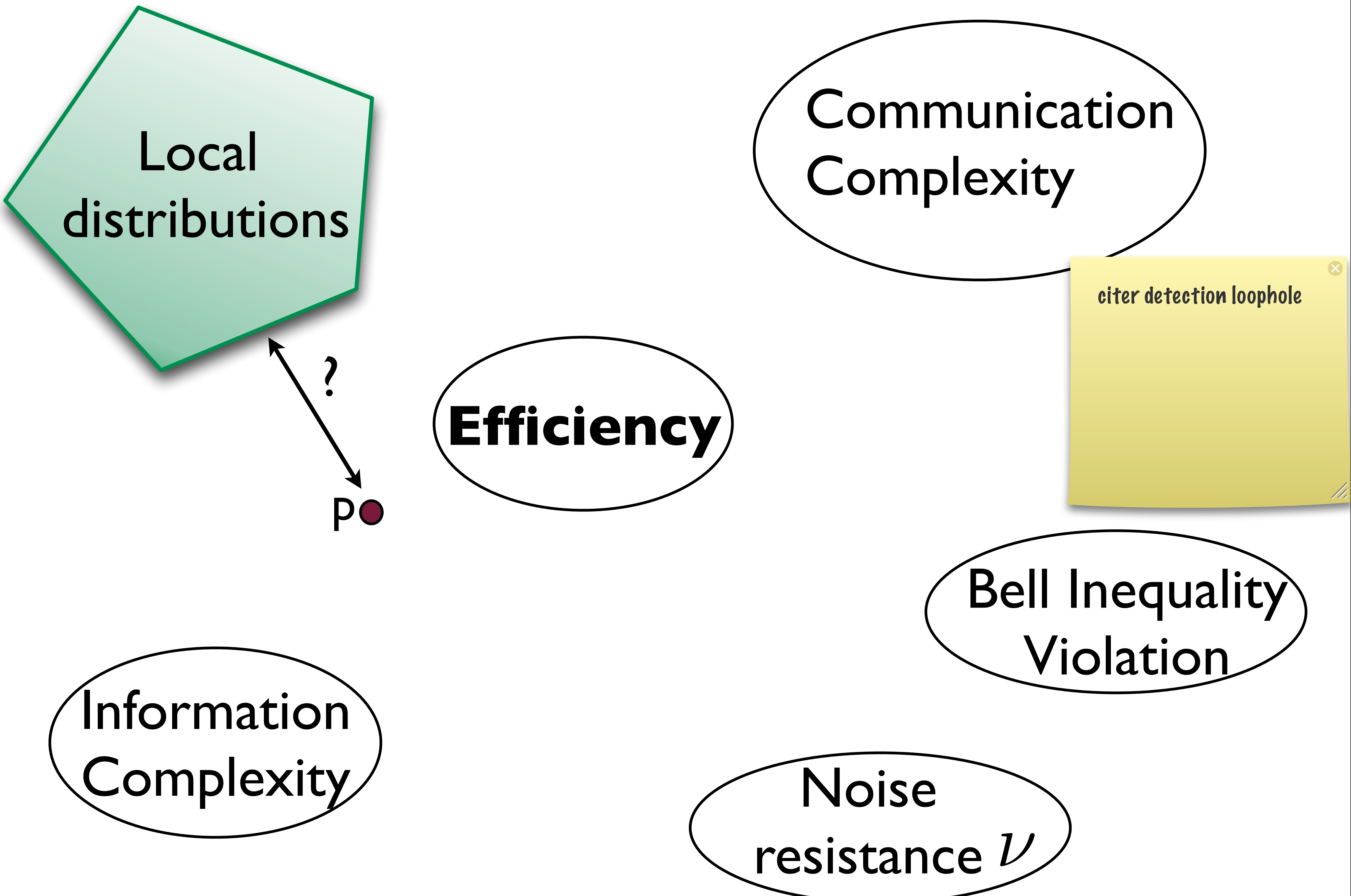
Bell tests and applications to communication and information complexity

I.Kerenidis, S. Laplante, V. Lerays, J. Roland, D. Xiao

LIAFA

Quantifying non locality



Bell Polytope [Bell69]

Local Hidden Variable

Alice

measurement: x
outcome: a

No communication

measurement: y
outcome: b

Bob

$$\text{s.t } a, b \sim p(a, b|x, y)$$

Bell Polytope [Bell69]

Shared Randomness

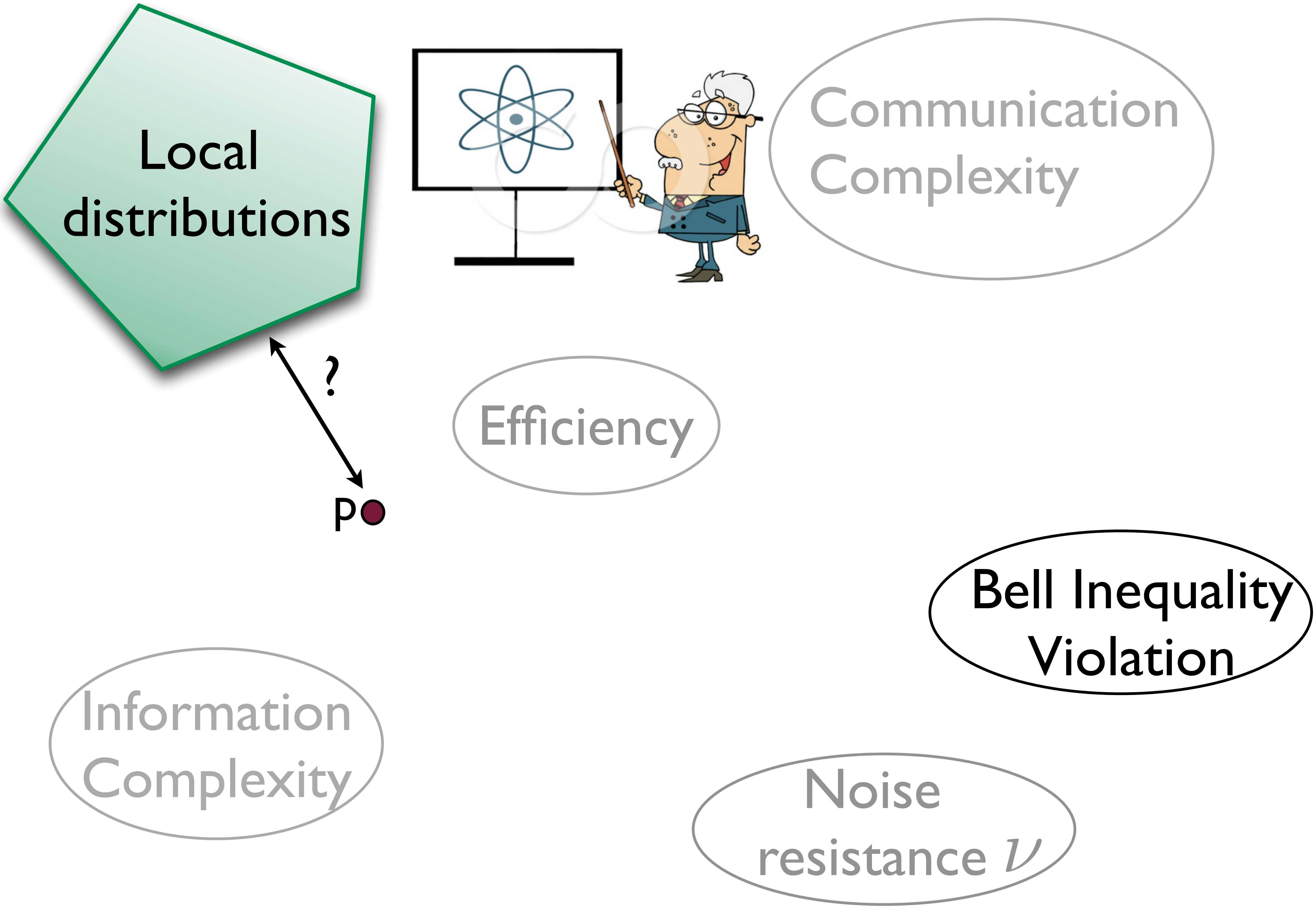
input: x
output: a

No communication

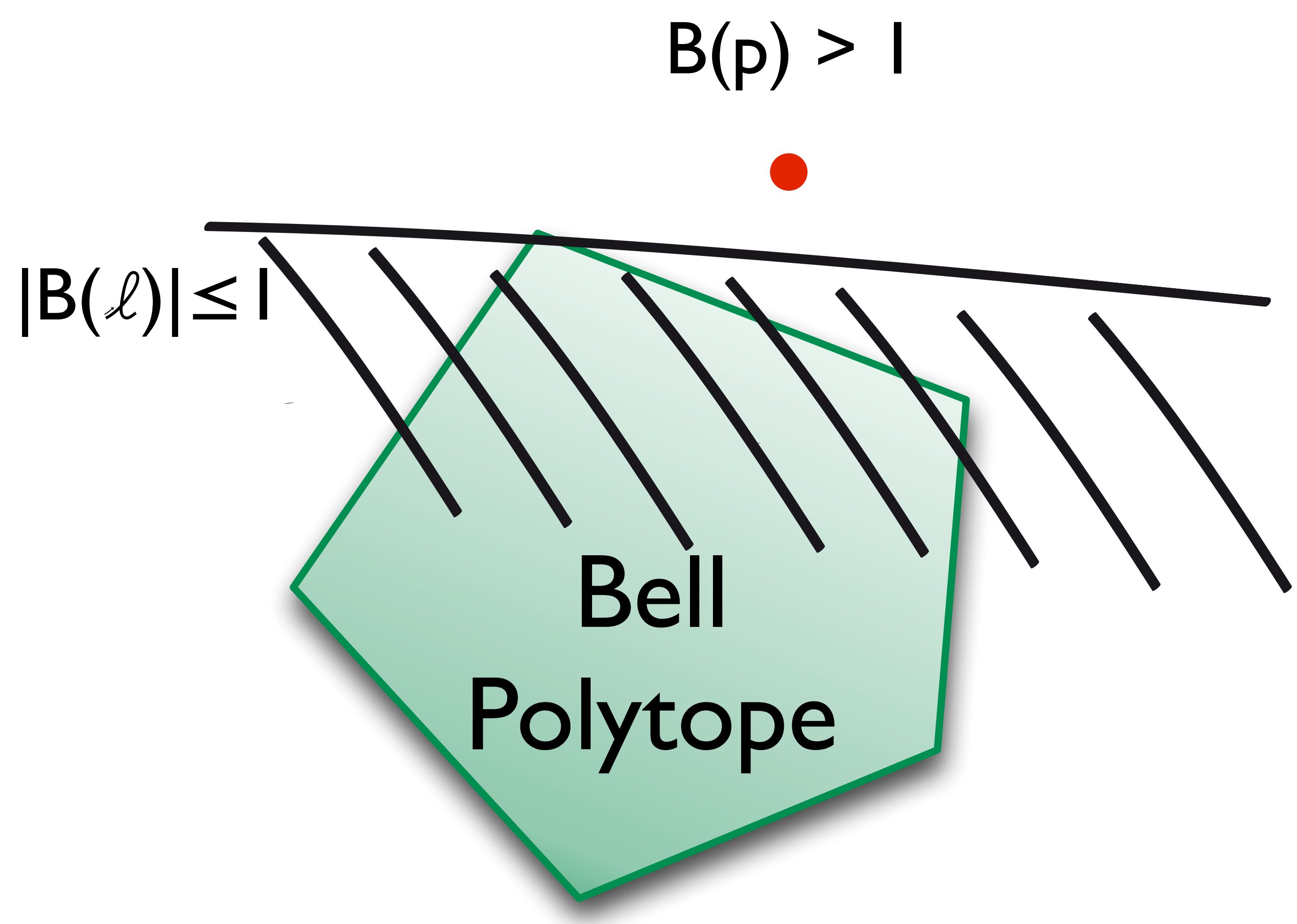
input: y
output: b

$$\text{s.t } a, b \sim p(a, b|x, y)$$

Quantifying non locality



Bell Inequality Violation



Bell inequality = linear function B s.t
$|B(l)| \leq 1$ for all local strategies l.

Quantifying non locality

Local distributions

Communication Complexity [Mau92]

?

P

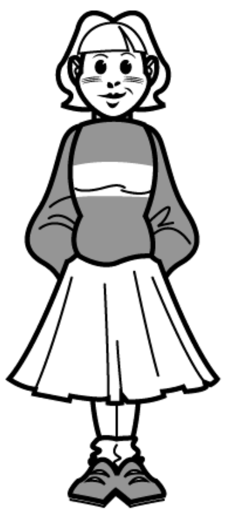
Efficiency

Bell Inequality Violation

Information Complexity

Noise resistance ν

Communication Complexity


Alice

input: x
output: a

Shared randomness

Communication

input: y
output: b

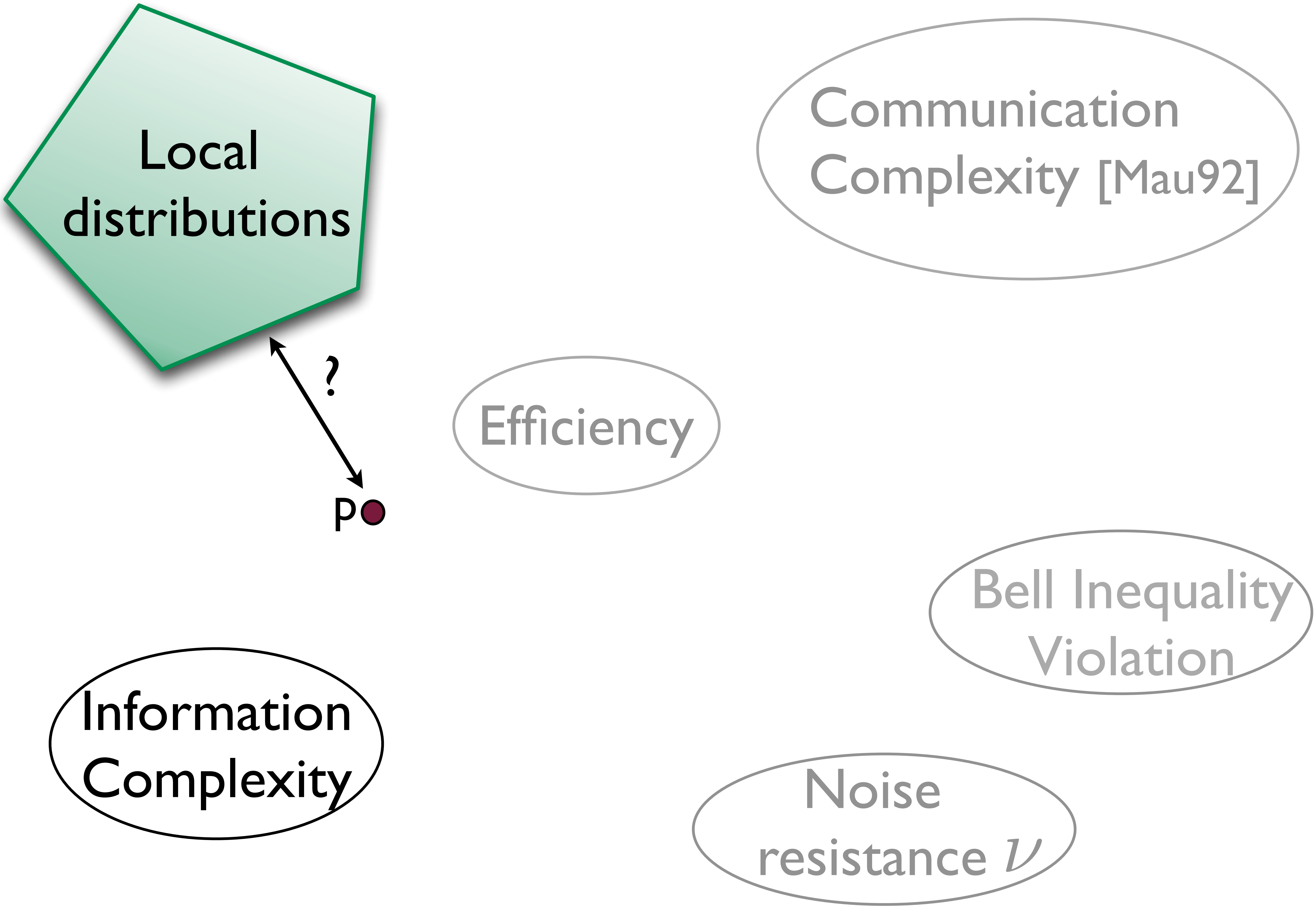

Bob

$$\text{s.t } a, b \sim p(a, b|x, y)$$

Cost(Π) = number of bits exchanged in protocol

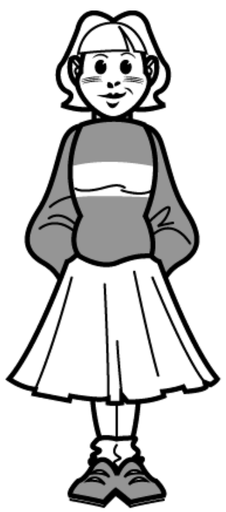
$$\boxed{R(p) = \inf_{\Pi \text{ simulates } p} Cost(\Pi)}$$

Quantifying non locality



Information Complexity

[CSWY01, BYJKS04, BBCR10]



Alice

input: x
output: a

$$x, y \sim \mu$$

Shared randomness

Information

s.t $a, b \sim p(a, b|x, y)$

input: y
output: b

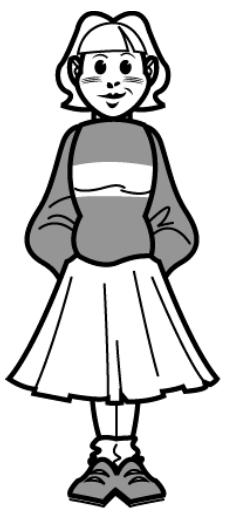
Bob

$IC_\mu(\Pi)$ = what Alice and Bob learn about the other input from Π .

$$\boxed{IC_\mu(p) = \inf_{\Pi \text{ simulates p}} IC_\mu(\Pi)}$$

Information Complexity

[CSWY01, BYJKS04, BBCR10]



Alice

input: x
output: a

$$x, y \sim \mu$$

Shared randomness

Information

s.t $a, b \sim p(a, b|x, y)$

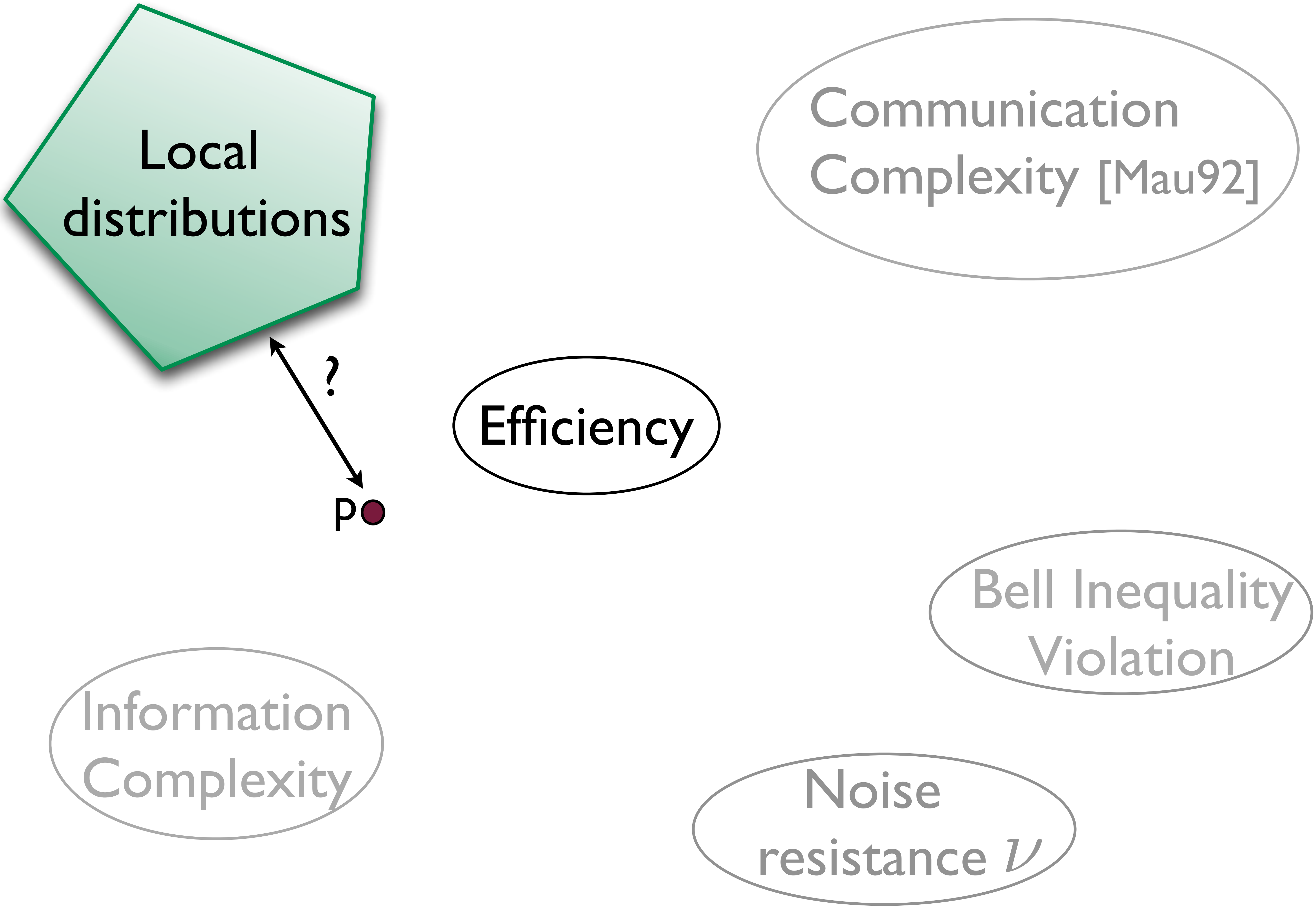
input: y
output: b

Bob

$$IC_\mu(\Pi) = I(T_\Pi; X|Y) + I(T_\Pi; Y|X)$$

$$IC_\mu(p) = \inf_{\Pi \text{ simulates p}} IC_\mu(\Pi)$$

Quantifying non locality

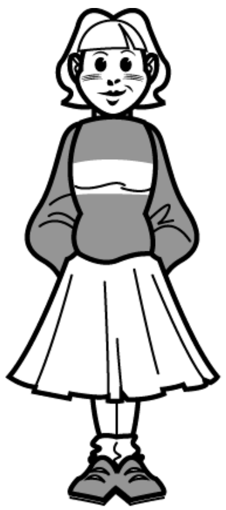


Efficiency (detection loophole)

$$x, y \sim \mu$$

Shared randomness λ

(LHV)



Alice

input: x

output: a or $\perp$

No communication

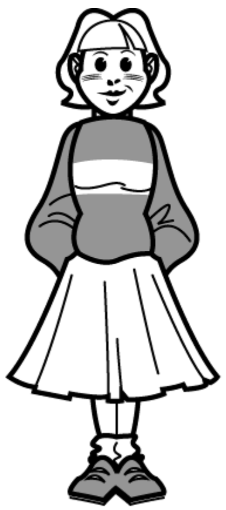
input: y

output: b or $\perp$

Bob

$$\text{Output} \begin{cases} a, b & \text{if } a \neq \perp \text{ and } b \neq \perp \\ \perp & otherwise \end{cases}$$

Efficiency (detection loophole)



Alice

$$x, y \sim \mu$$

Shared randomness λ

(LHV)

input: x

output: a or $\perp$

No communication

input: y

output: b or $\perp$

Bob

$$\text{Output} \begin{cases} a, b & \text{if } a \neq \perp \text{ and } b \neq \perp \\ \perp & otherwise \end{cases}$$

efficiency η:

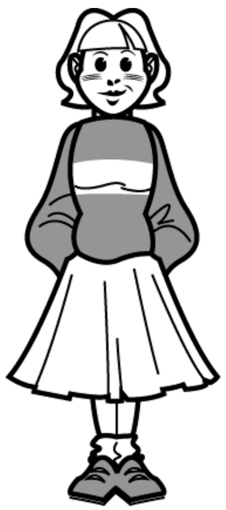
$$\forall (x,y), \eta = \mathbb{P}_\lambda[\Pi(x,y) \neq \perp]$$

Efficiency (detection loophole)

$$x, y \sim \mu$$

Shared randomness λ

(LHV)



input: x

output: a or $\perp$

No communication

input: y

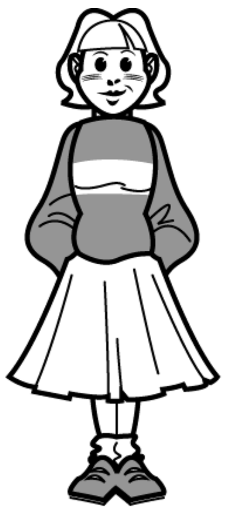
output: b or $\perp$

Output $\begin{cases} a, b & \text{if } a \neq \perp \text{ and } b \neq \perp \\ \perp & otherwise \end{cases}$

efficiency η: $$\forall (x,y), \eta = \mathbb{P}_\lambda[\Pi(x,y) \neq \perp]$$

correct : $$\mathbb{P}_{(x,y)\sim\mu,\lambda}[\Pi(x,y) = a, b | \Pi(x,y) \neq \perp] = p(a,b|x,y)$$

Efficiency (detection loophole)



Alice

$$x, y \sim \mu$$

Shared randomness λ

(LHV)

input: x

output: a or $\perp$

No communication

input: y

output: b or $\perp$

Bob

$$\text{Output} \begin{cases} a, b & \text{if } a \neq \perp \text{ and } b \neq \perp \\ \perp & otherwise \end{cases}$$

efficiency η:

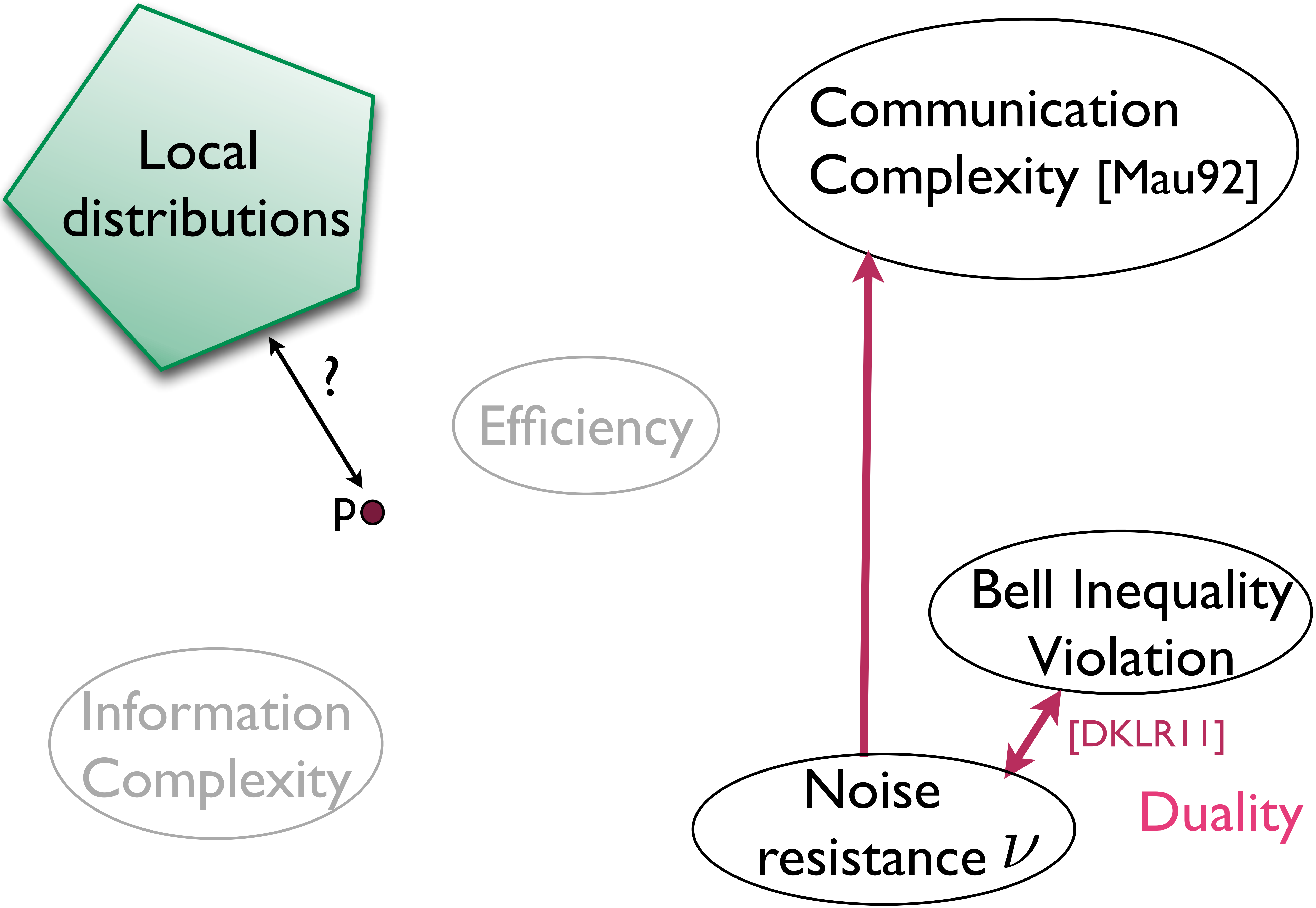
$$\forall (x, y), \eta = \mathbb{P}_\lambda[\Pi(x, y) \neq \perp]$$

correct :

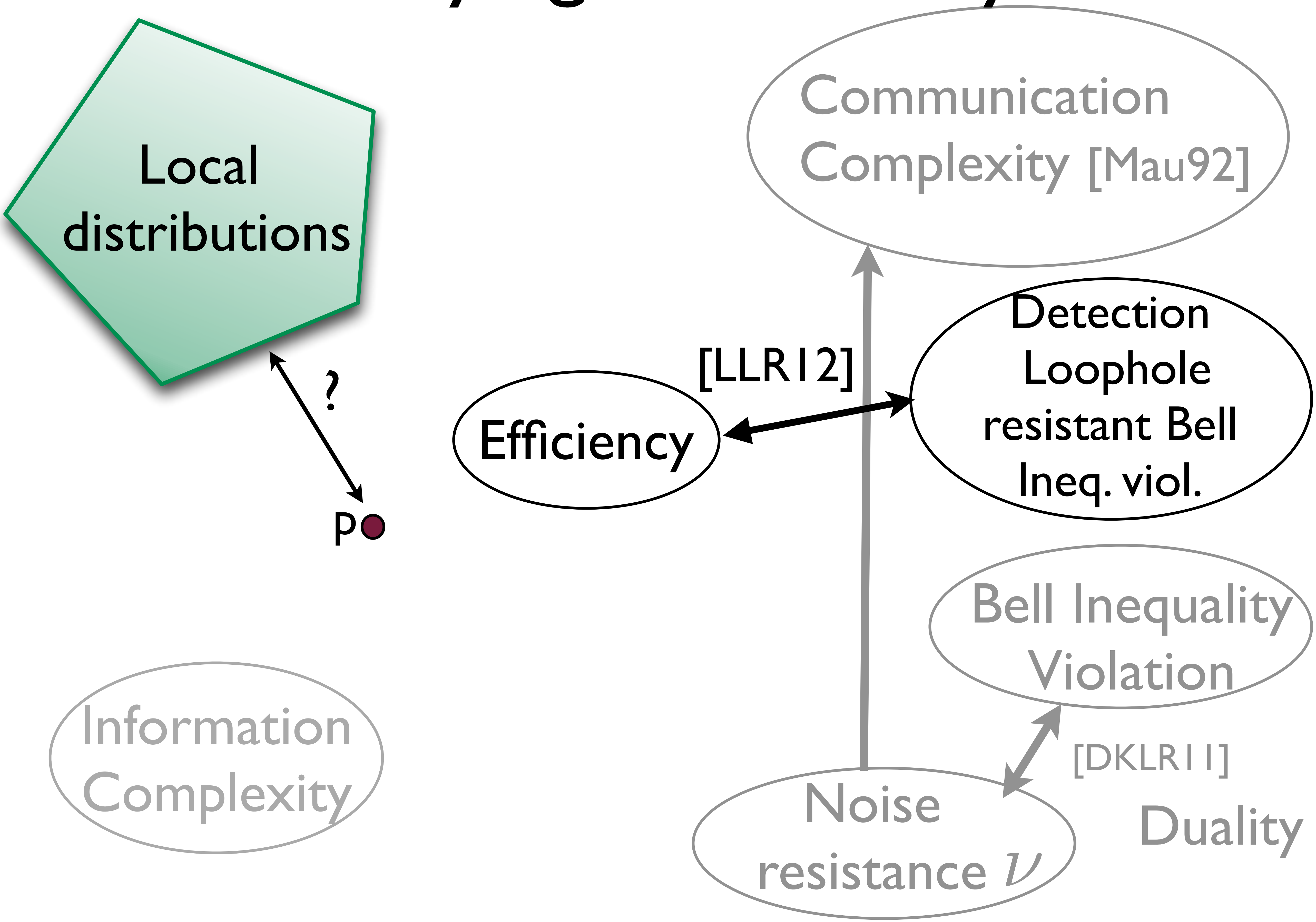
$$\mathbb{P}_{(x,y)\sim\mu,\lambda}[\Pi(x, y) = a, b | \Pi(x, y) \neq \perp] = p(a, b|x, y)$$

<u>Def</u>: If η is the maximum efficiency achieved by local protocol which computes p; then $\text{eff}(p) = \frac{1}{\eta}$

Quantifying non locality



Quantifying non locality



Detection Loophole resistant Bell inequalities

The efficiency bound is the optimal value of a linear program.

$$\min\{1/\eta : \exists l \in \mathcal{L}^{\perp} \text{ for p with efficiency } \eta\}$$

Dual: maximal Bell inequality violation

$$\max\{B(p) : B(l) \leq 1, \forall l \in \mathcal{L}^{\perp}\}$$

Local strategies where players can abort

Exponential violation

Thm[JPPG+10]: For any p which can be simulated using an n-dimensional shared quantum state and for any B s.t. $|B(l)| \leq 1, \forall l \in \mathcal{L}$ then $B(p) \leq O(n)$.

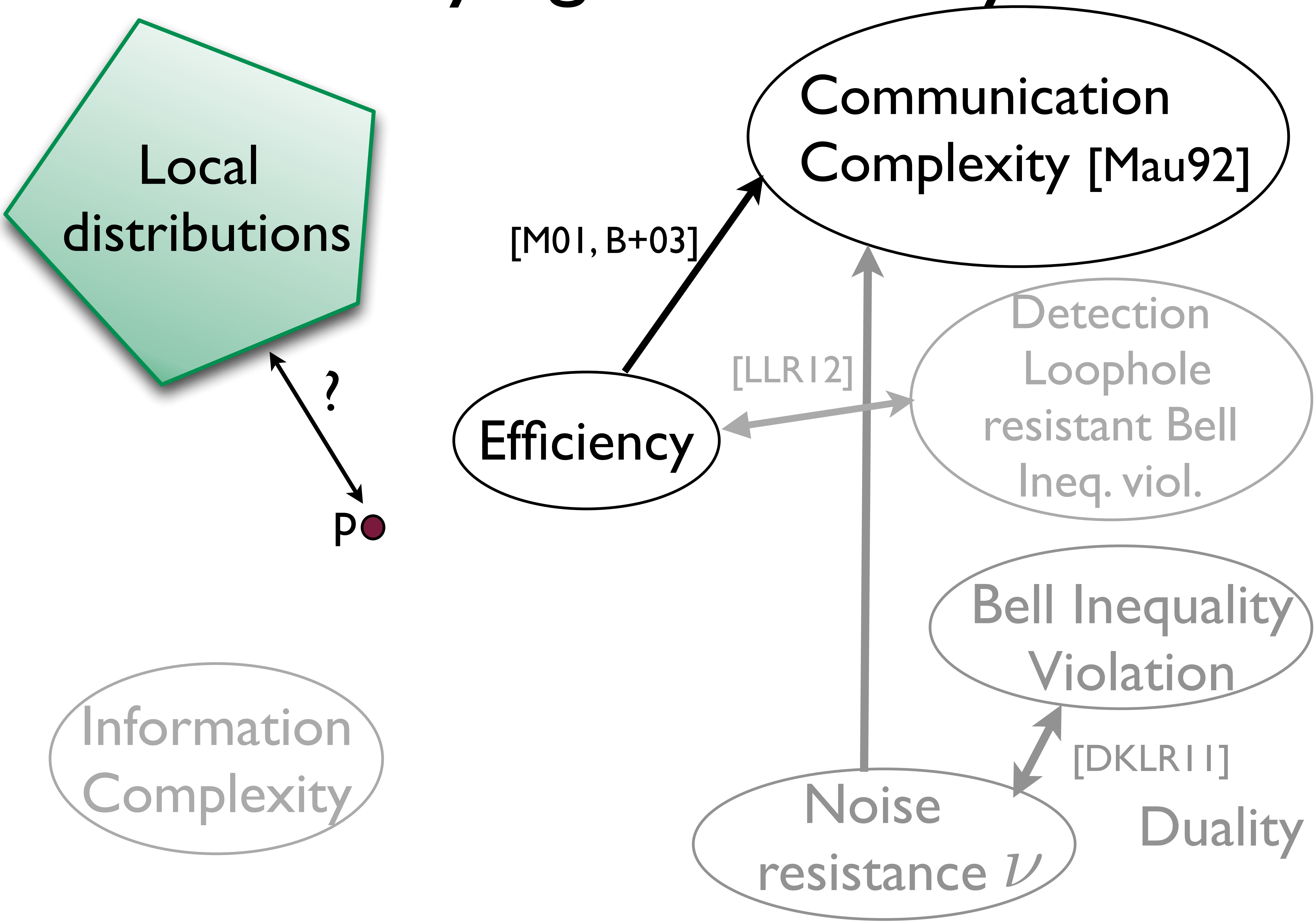
but there exists such p, B and C s.t. $B(l) \leq 1, \forall l \in \mathcal{L}^{\perp_A}$ and $B(p) \geq \frac{2^{\frac{\sqrt{n-1}}{2C}}}{n}$

[LLR12]

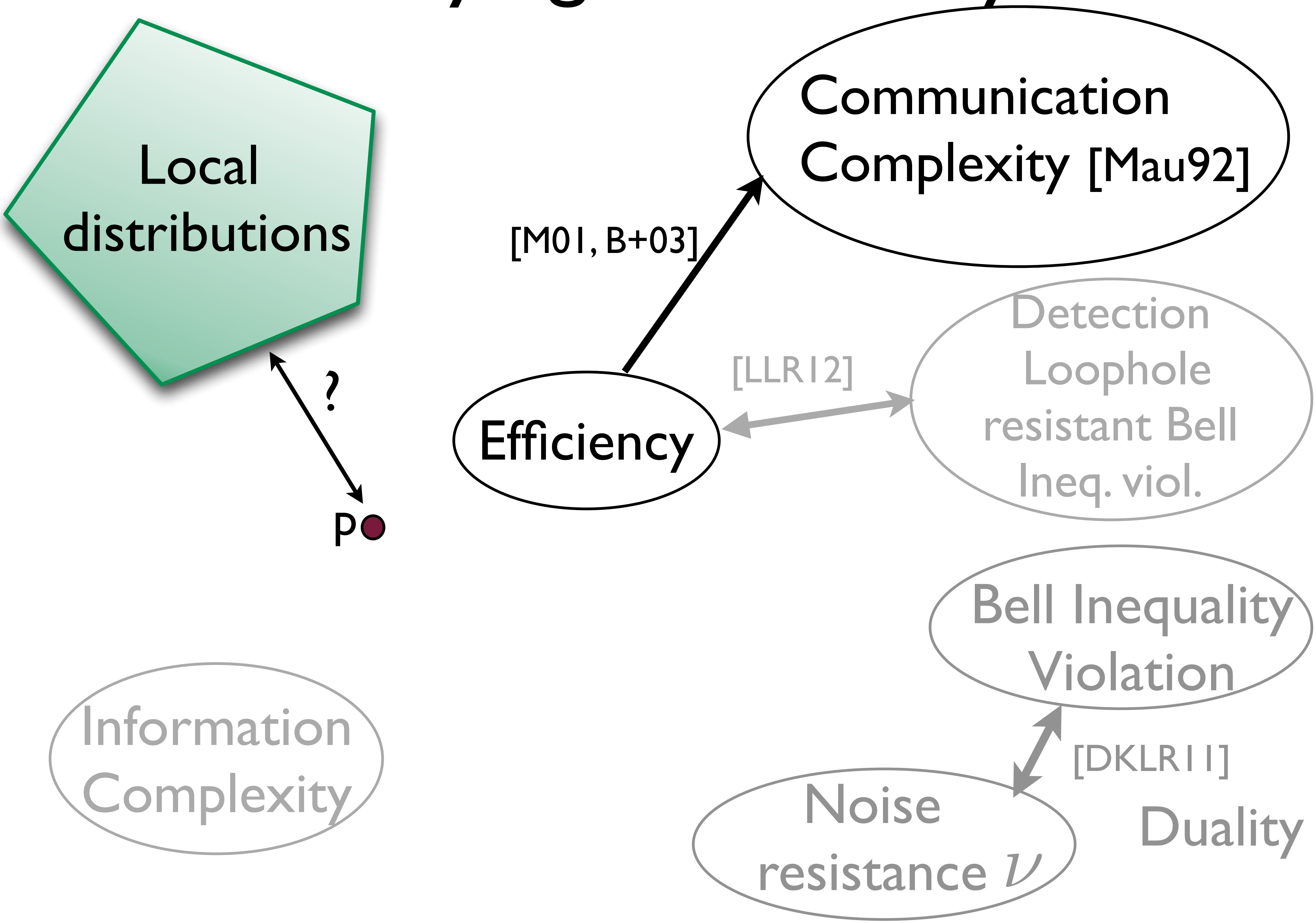
one way case

p is based on Hidden Matching [BJK04,BRSdW11]

Quantifying non locality



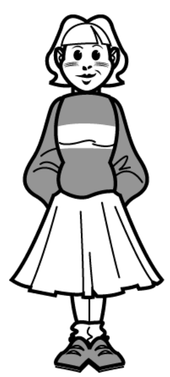
Quantifying non locality



Efficiency lower bound on CC

Theorem: [M01, BHMR03]
Given a protocol Π using c bits of communication for p, we can construct a local protocol for p with efficiency $\eta = 2^{-c}$.

Proof:



Alice

x

Using shared randomness, pick a random conversation M$\in \{0,1\}^c$

y

Bob

M on x if M is consistent with x;
$\perp$ otherwise

M on y if M is consistent with y;
$\perp$ otherwise

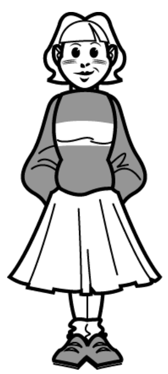
efficiency = 2^{-c} independent of (x,y)
correctness = conditioned on non aborting, same as Π

Efficiency lower bound on CC

Def: If η is the maximum efficiency achieved by a local protocol which computes p; then $\mathrm{eff}(p) = \frac{1}{\eta}$.

Thm: $\log(\mathrm{eff}(p)) \leq R(p)$

Proof:



Alice

x

y

Bob

Using shared randomness, pick a random conversation M$\in \{0,1\}^c$

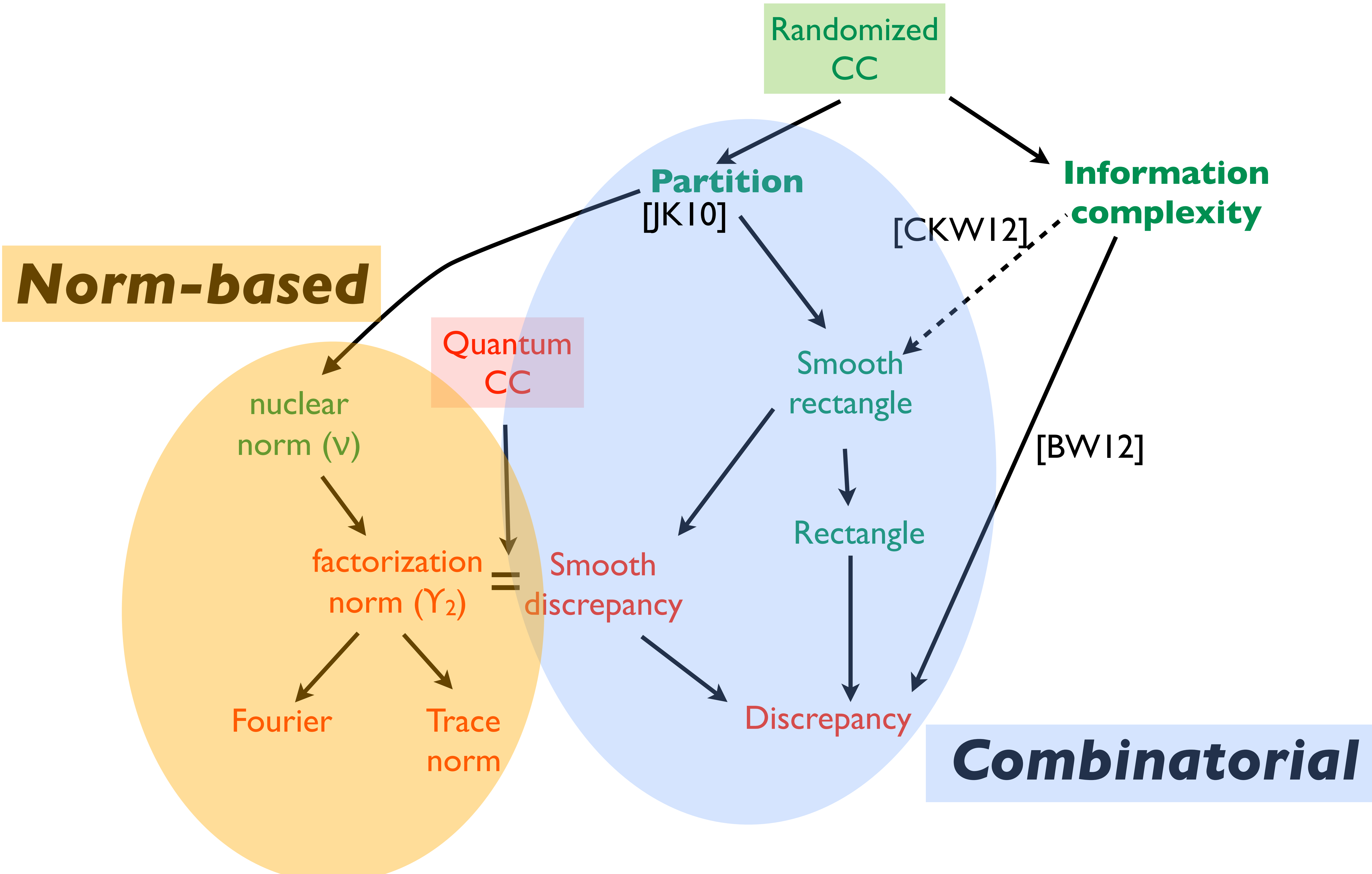
M on x if M is consistent with x;
$\perp$ otherwise

M on y if M is consistent with y;
$\perp$ otherwise

efficiency = 2^{-c} independent of (x,y)

correctness = conditioned on non aborting, same as Π

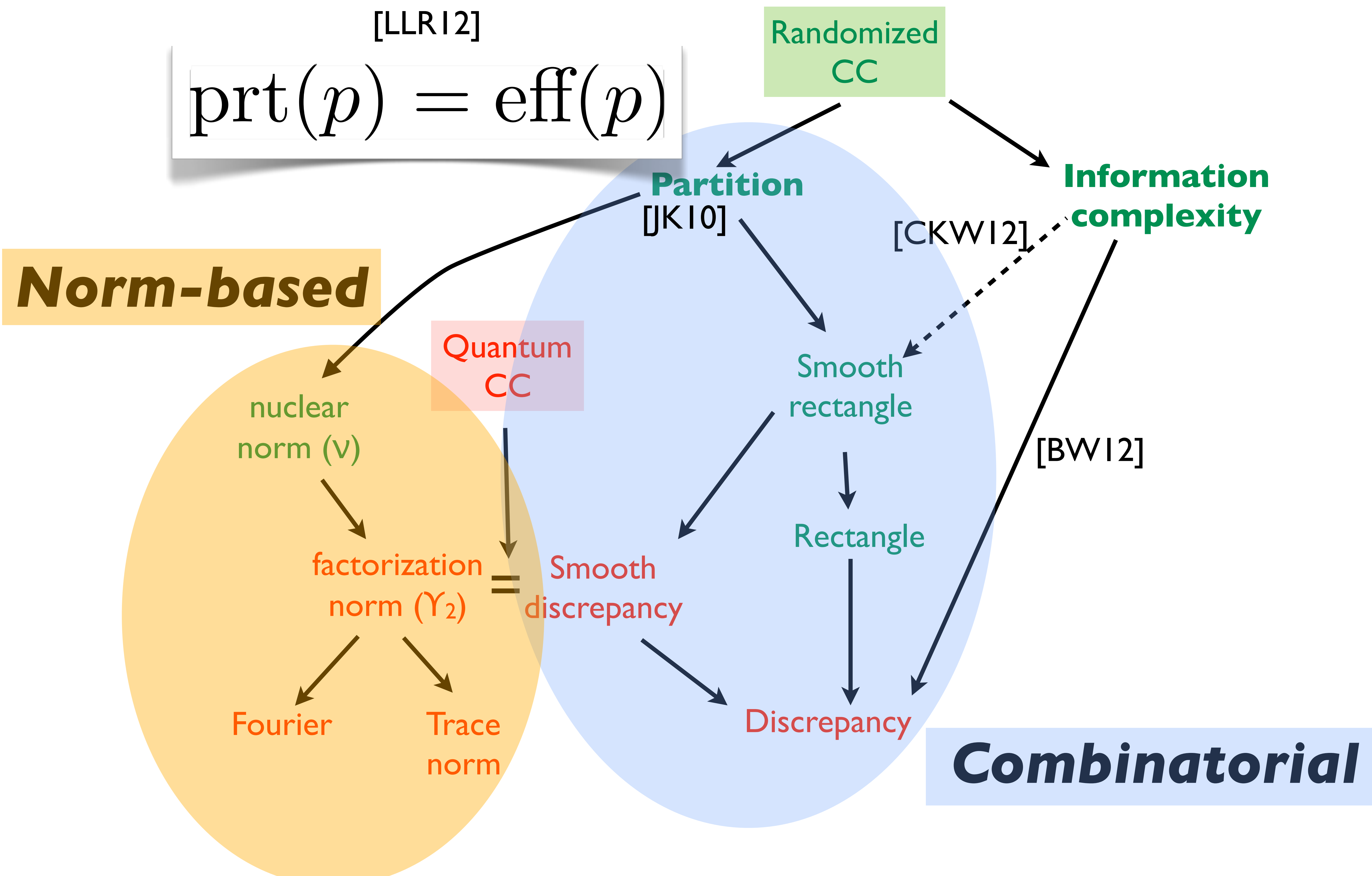
Communication lower bounds



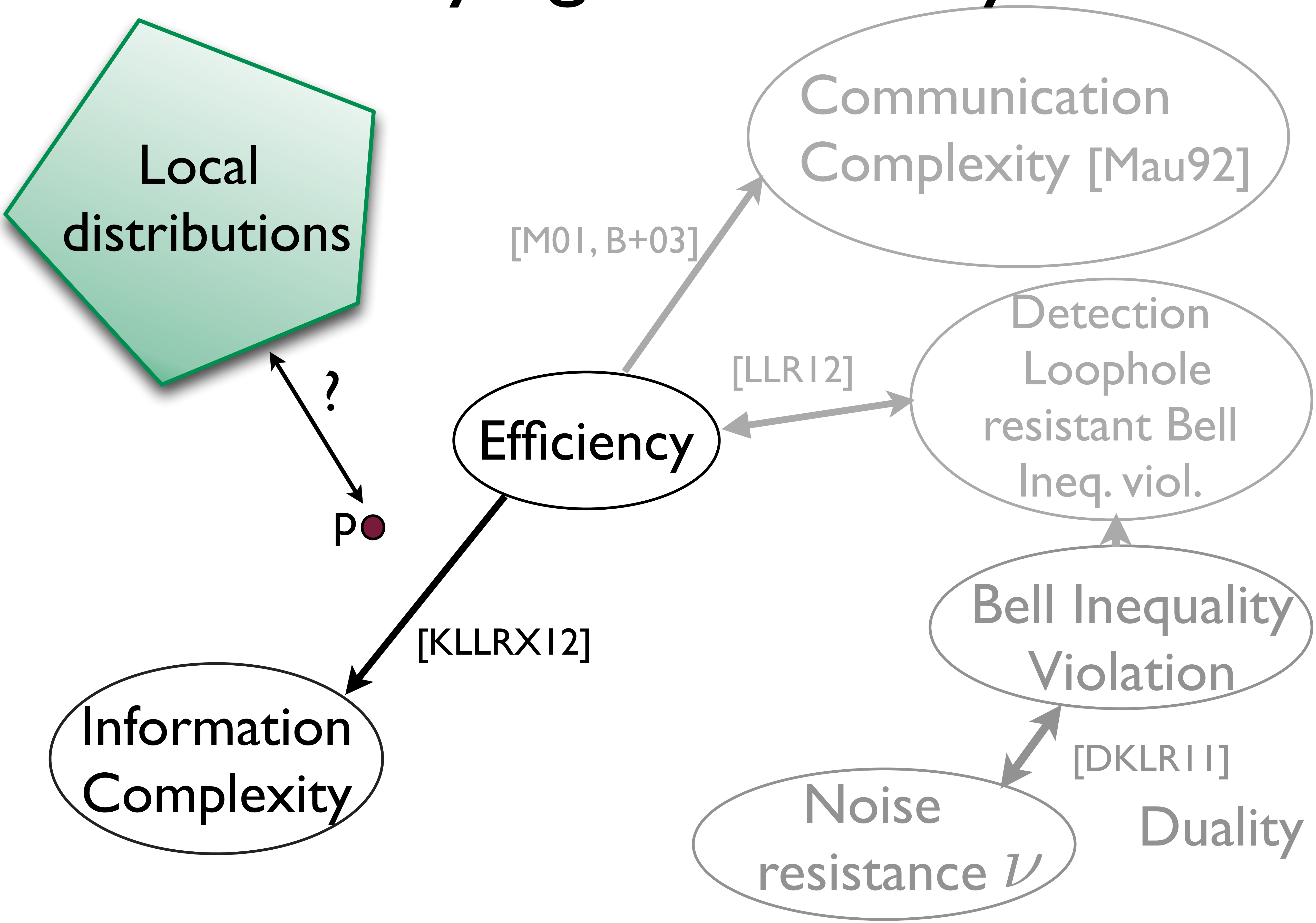
Communication lower bounds

[LLR12]

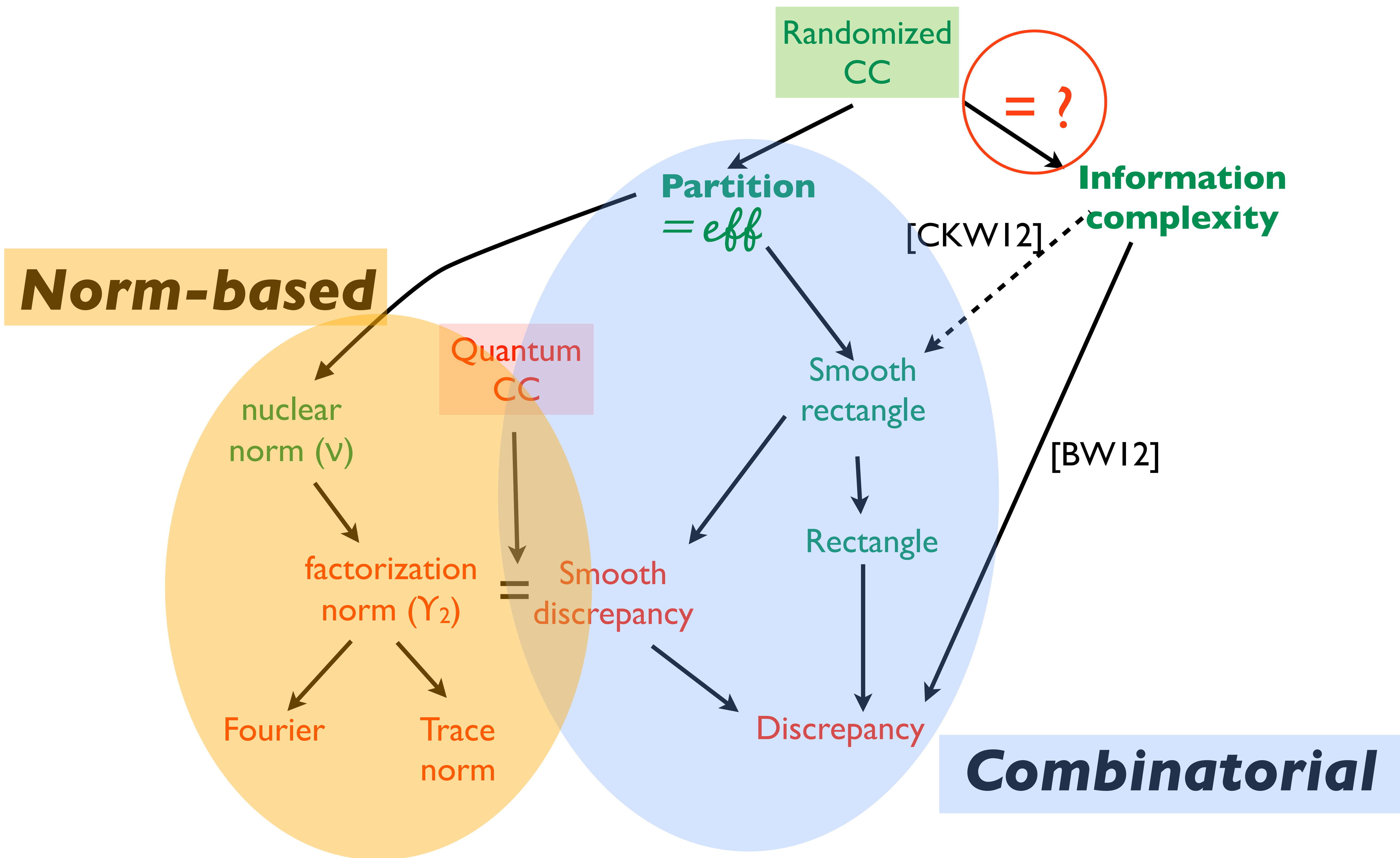
$$\mathrm{prt}(p) = \mathrm{eff}(p)$$



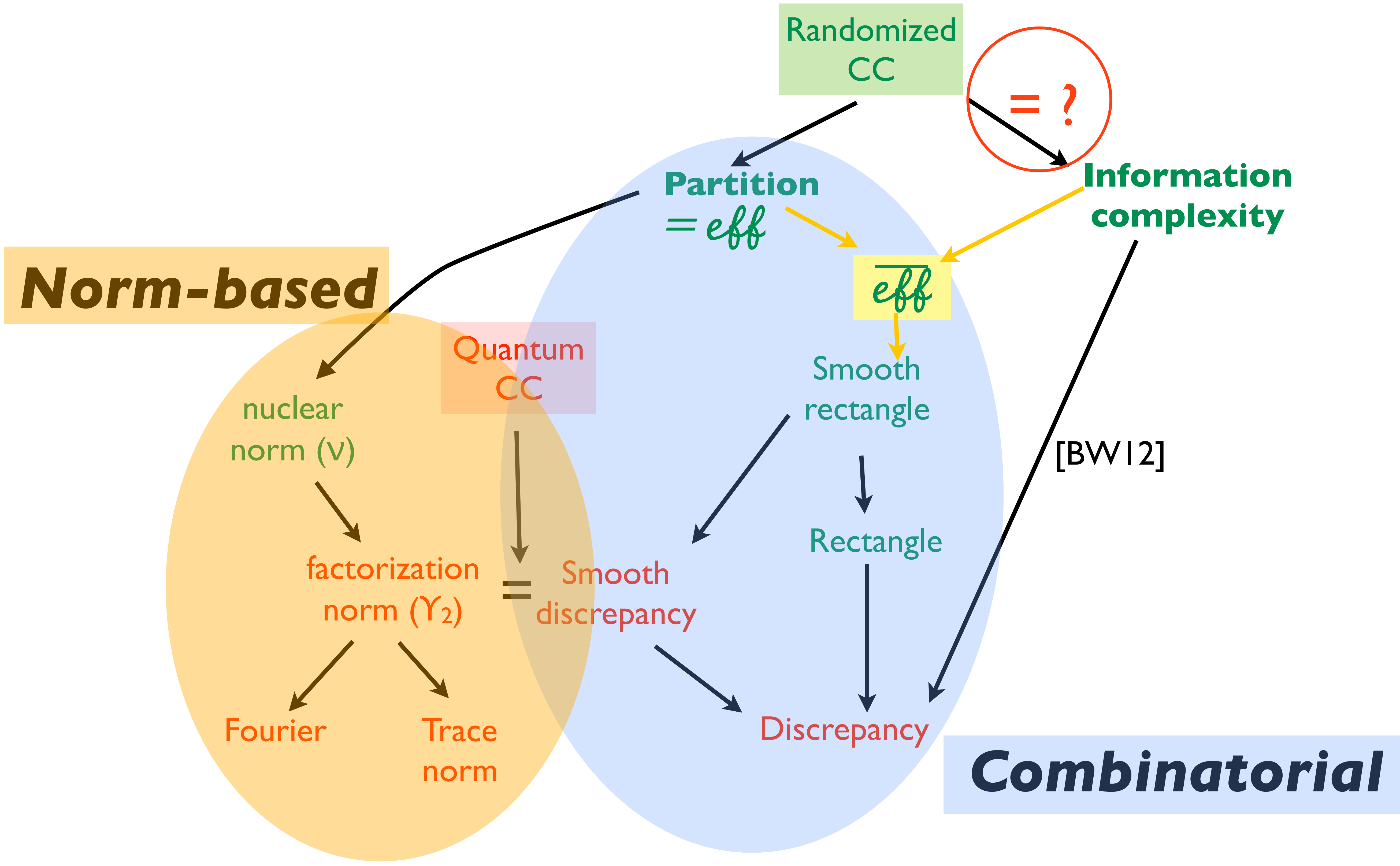
Quantifying non locality



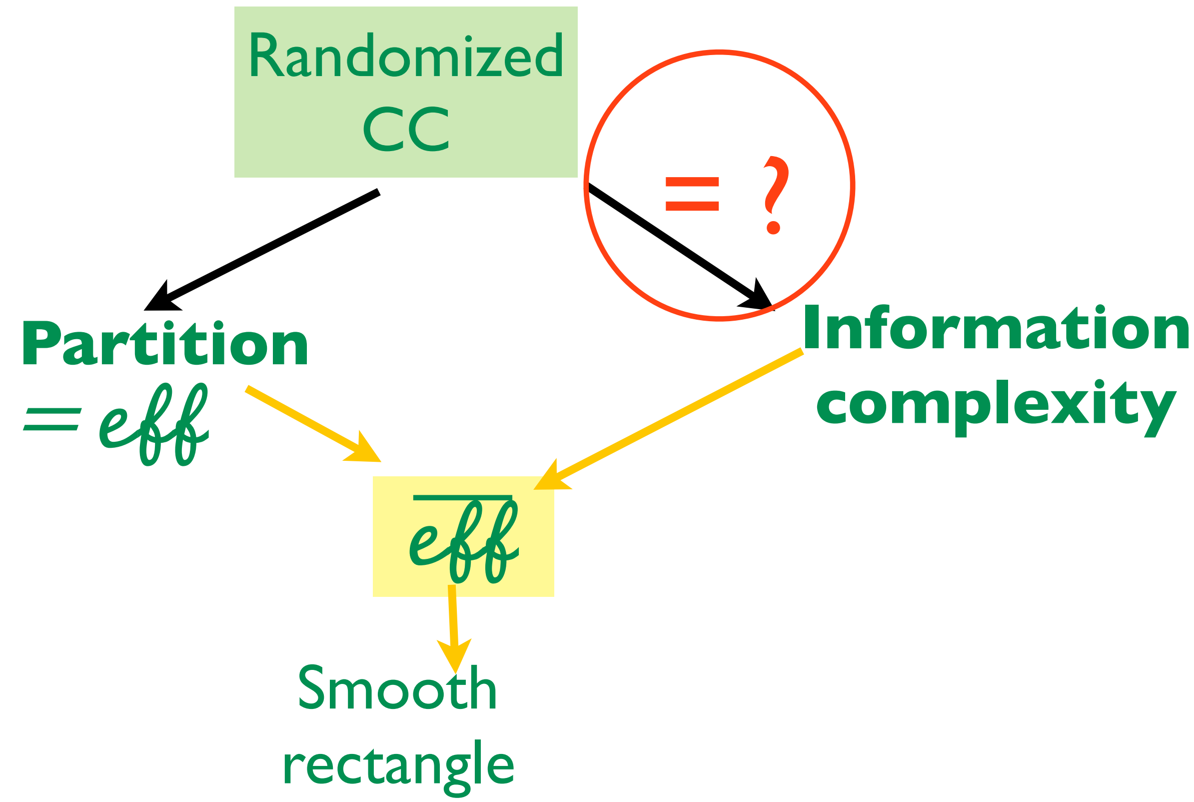
Efficiency lower bound on IC



Efficiency lower bound on IC



Efficiency lower bound on IC



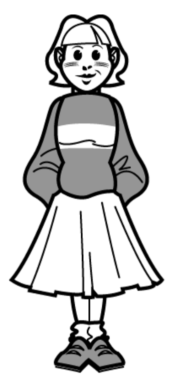
Def: relaxed efficiency = $\min\{1/\eta : \exists l \in \mathcal{L}^{\perp}$ computing p with efficiency η_{xy} s.t $\forall xy, (1-\epsilon)\eta \leq \eta_{xy} \leq \eta\}$

Efficiency lower bound on IC

<u>Def</u>: If η is the maximum efficiency achieved by a local protocol which computes p; then $\text{eff}(p) = \frac{1}{\eta}$.

<u>Thm</u>: $\log(\text{eff}(p)) \leq R(p)$

<u>**Proof:**</u>


Alice

x

Using shared randomness, pick a random conversation M$\in \{0,1\}^c$

y


Bob

M on x if M is consistent with x;
$\perp$ otherwise

M on y if M is consistent with y;
$\perp$ otherwise

efficiency = 2^{-c} independent of (x,y)

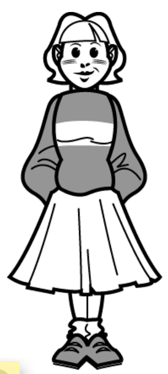
correctness = conditioned on non aborting, same as Π

Efficiency lower bound on IC

Def: If η is the maximum efficiency achieved by a local protocol which computes p; then $\mathrm{eff}(p) = \frac{1}{\eta}$.

Thm: $\log(\mathrm{eff}(p)) \leq \cancel{R(p)}\ O(IC(p))$

Proof:



Alice

x

y

Bob

but IC can be much smaller so more difficult to lower bound.
The proof uses sophisticated correlated rejection sampling techniques

Improve to obtain

$$\eta = 2^{-O(IC(p))}$$

Using sampling from [BW12]

Application: exponential separation between quantum CC and classical IC

Problem 3. *What is the relationship between* $Q(f,\varepsilon)$ *and* $\mathsf{IC}\,(f,\varepsilon)$*?*
In particular are there problems for which $Q(f,\varepsilon) = O(\mathrm{polylog}(\mathsf{IC}\,(f,\varepsilon)))$*?*

[Bra12]

Application: exponential separation between quantum CC and classical IC

Problem 3. *What is the relationship between* $Q(f, \varepsilon)$ *and* $\mathsf{IC}(f, \varepsilon)$*?*
In particular are there problems for which $Q(f, \varepsilon) = O(\text{polylog}(\mathsf{IC}(f, \varepsilon)))$*?*

[Bra12]

[KR11,KLLRX12]

$\overline{\text{eff}}(VSP_n) = \Omega(exp(n^{\frac{1}{3}}))$

So, $IC(VSP_n) \geq \log(\overline{\text{eff}}(VSP_n)) = \Omega(n^{\frac{1}{3}})$

Application: exponential separation between quantum CC and classical IC

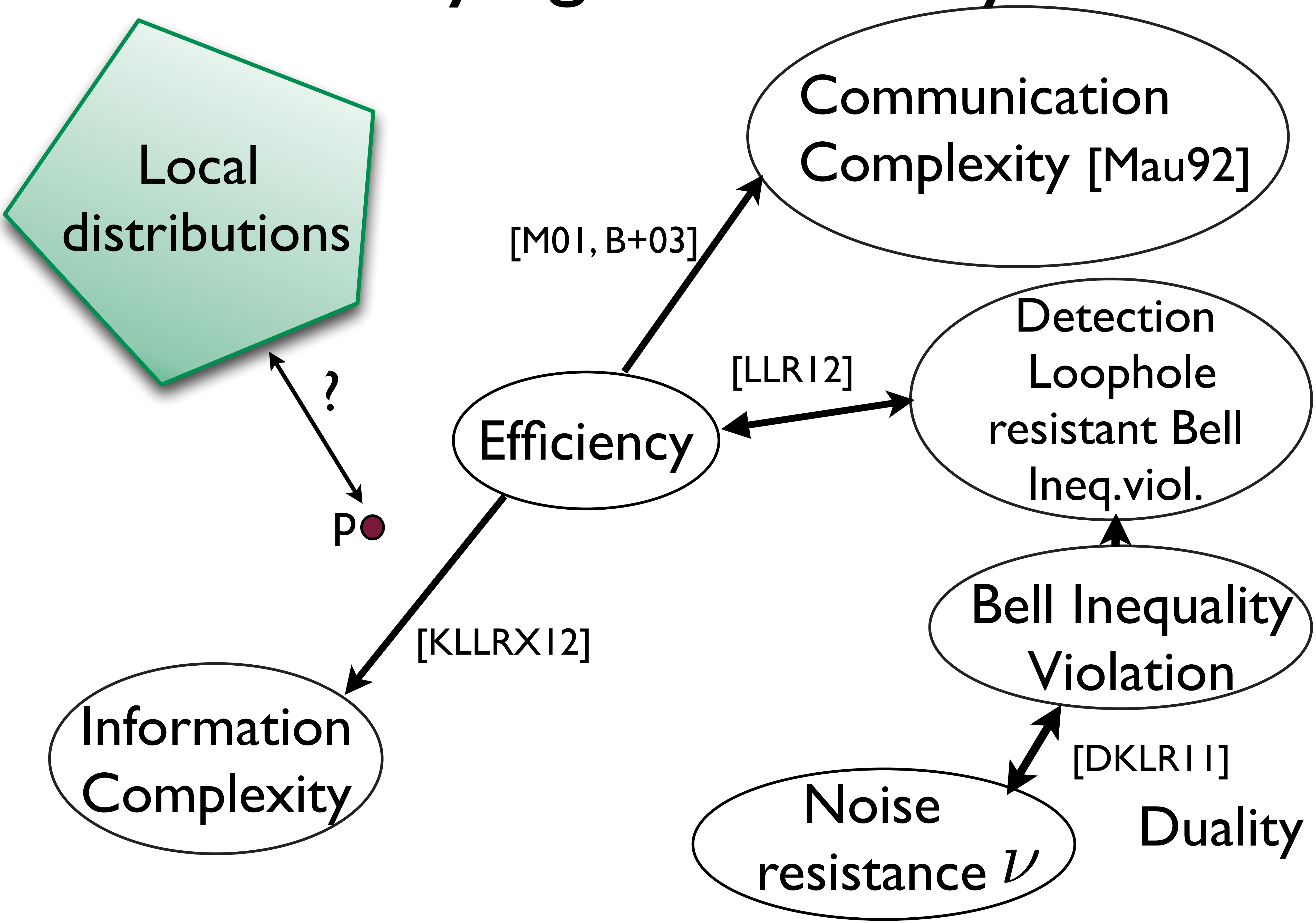
Problem 3. *What is the relationship between* $Q(f,\varepsilon)$ *and* $\mathsf{IC}\,(f,\varepsilon)$*?*
In particular are there problems for which $Q(f,\varepsilon) = O(\mathrm{polylog}(\mathsf{IC}\,(f,\varepsilon)))$*?*

[Bra12]

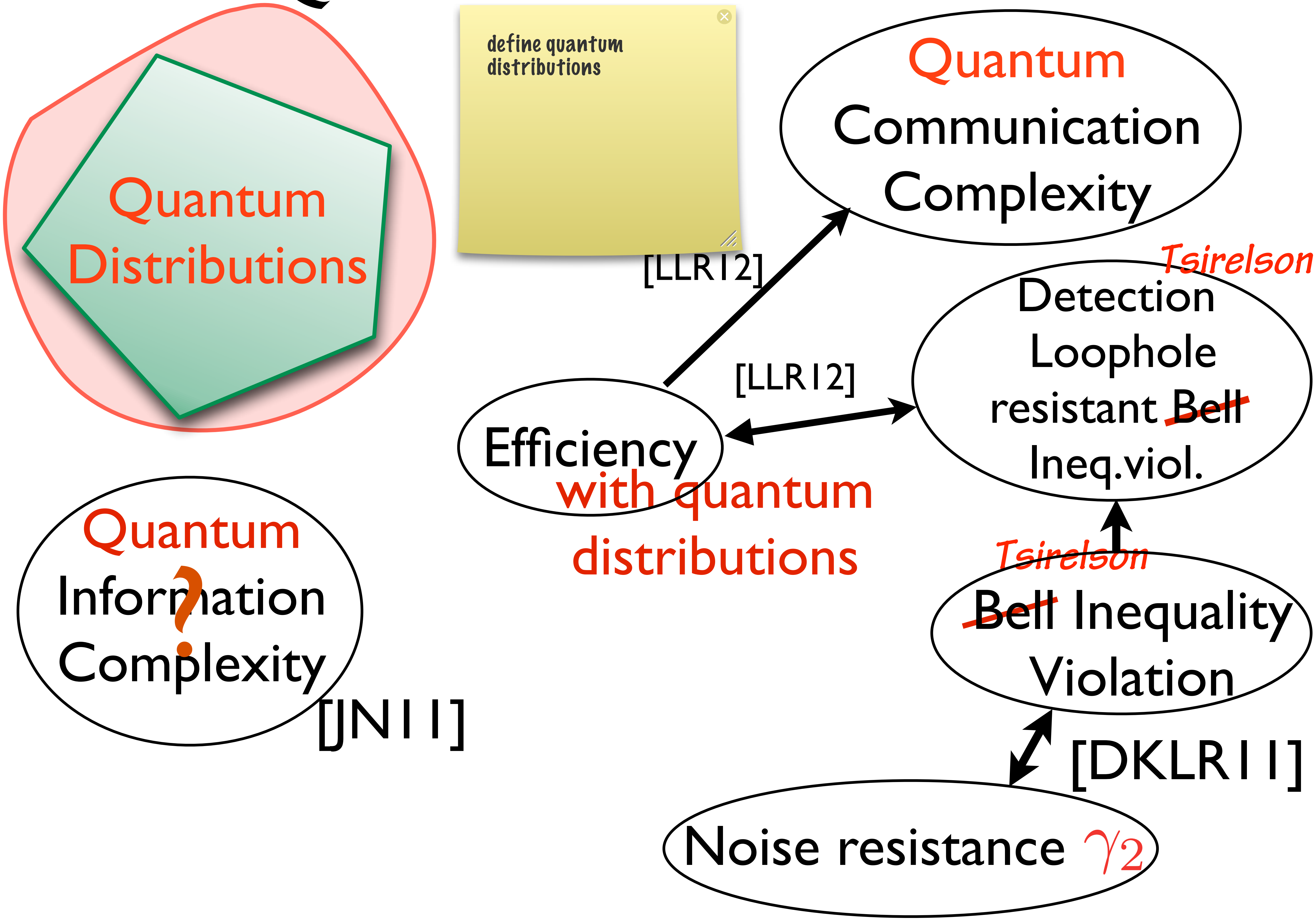
$$\boxed{\begin{aligned} IC(VSP_n) &= \Omega(n^{\frac{1}{3}}) \\ Q^{\rightarrow}(VSP_n) &= O(\log(n)) \end{aligned}}$$

[Raz99]

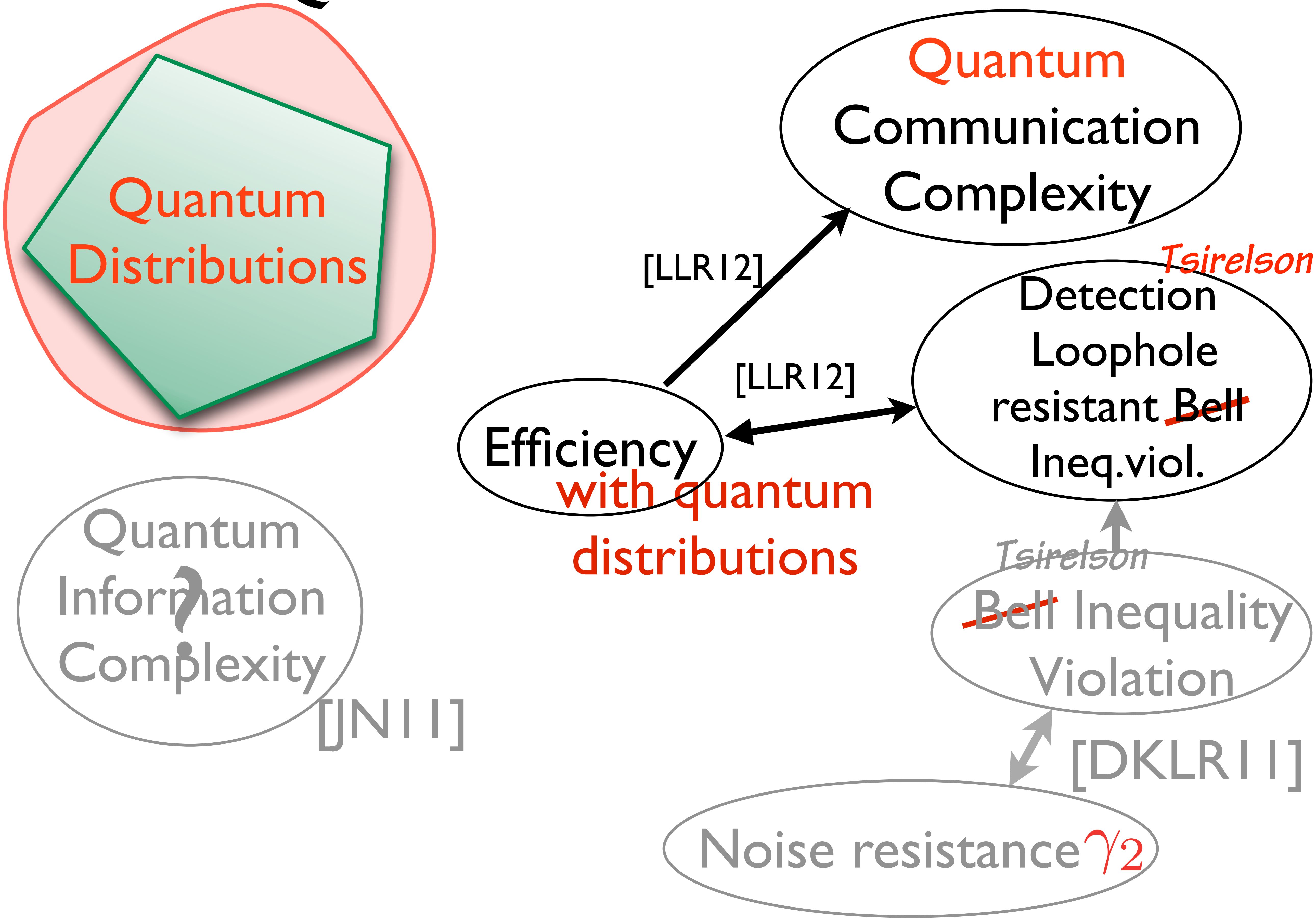
Quantifying non locality



Quantum Extension



Quantum Extension

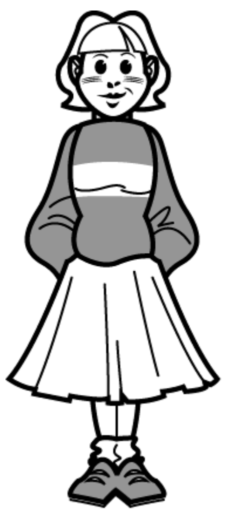


eff*

Zero communication protocol $\Pi \in \mathcal{Q}^{\perp}$

$x, y \sim \mu$

Shared randomness λ



Shared quantum state

input: x
output: a or $\perp$

No communication

input: y
output: b or $\perp$

Output $\begin{cases} a, b & \text{if } a \neq \perp \text{ and } b \neq \perp \\ \perp & otherwise \end{cases}$

efficiency : $\forall (x,y), \eta = \mathbb{P}_{\lambda}[\Pi(x,y) \neq \perp]$

correct : $\mathbb{P}_{(x,y)\sim\mu,\lambda}[\Pi(x,y) = a,b | \Pi(x,y) \neq \perp] = p(a,b|x,y)$

Def: $\text{eff}^*(p) = \min\{1/\eta : \exists q \in Q^{\perp} \text{ for p with efficiency } \eta\}$

Thm: $Q(p) \geq \log(\text{eff}^*(p)) \geq \log(\gamma_2(p))$

Quantum CC

eff*

Quantum
efficiency
bound

<u>Def:</u> $\mathrm{eff}^*(p) = \min\{1/\eta : \exists q \in Q^\perp \text{ for p with efficiency } \eta\}$

<u>Thm:</u> $Q(p) \geq \log(\mathrm{eff}^*(p)) \geq \log(\gamma_2(p))$

eff*

Quantum efficiency bound

<u>Def</u>: $\mathrm{eff}^*(p) = \min\{1/\eta : \exists q \in Q^\perp \text{ for p with efficiency } \eta\}$

<u>Thm:</u> $Q(p) \geq \log(\mathrm{eff}^*(p)) \geq \log(\gamma_2(p))$

- One-way variant is tight (up to small error): only Alice can abort.

<u>Thm</u>: $Q^{\rightarrow}(p) \leq O(\log(\mathrm{eff}^{*\rightarrow}(p))) + \log(\log(1/\epsilon))$

eff*

Quantum efficiency bound

$\underline{\text{Def}}$: $\mathrm{eff}^*(p) = \min\{1/\eta : \exists q \in Q^\perp \text{ for p with efficiency } \eta\}$

$\underline{\text{Thm}}$: $Q(p) \geq \log(\mathrm{eff}^*(p)) \geq \log(\gamma_2(p))$

- One-way variant is tight (up to small error): only Alice can abort.

$\underline{\text{Thm}}$: $Q^\rightarrow(p) \leq O(\log(\mathrm{eff}^{*\rightarrow}(p))) + \log(\log(1/\epsilon))$

- Dual Formulation: Maximal Tsirelson inequality violation

$$\mathrm{eff}^*(\mathrm{p}) = \max\{B(p) : B(q) \leq 1, \forall q \in Q^\perp\}$$

Summary

- Efficiency bound is a strong lower bound for CC
- New strong lower bound for quantum CC
- New strong lower bound for IC
- Exponential separation between classical CC and quantum IC
- Efficiency equivalent to Detection Loophole resistant Bell (Tsirelson) inequality violation
- Exponential Detection Loophole Bell Inequality Violation

Open Questions

- Does IC = CC?
- Does eff = CC? Does eff* = QCC?
- New quantum CC lower bound using eff*?
- Direct sum for eff?
- Other exponential Bell Inequality Violations?

Thank you

Laplante, Lerays, Roland
"Classical and quantum partition bound and detector inefficiency",
ICALP 2012. quant-ph 1203.4155

Kerenidis, Laplante, Lerays, Roland, Xiao
"Lower bounds on information complexity via zero-communication protocols an applications",
FOCS 2012.quant-ph 1204.1505