Title: Modulation, Coding and Decoding for Classical-Quantum Channel

Date: Jun 26, 2008 03:00 PM

URL: http://pirsa.org/08060201

Abstract:

Modulation, coding and decoding for classical-quantum channel

- Toward realization of optical quantum communications -

T. S. Usuda

Aichi Prefectural University

June 26, 2008

Modulation, coding and decoding for classical-quantum channel

- Toward realization of optical quantum communications -

T. S. Usuda

Aichi Prefectural University

June 26, 2008

Prof. Hirota & me

very very long story

Dr. Fuchs' Joke

Dr. Fuchs' Joke

Osama Hirota

Dr. Fuchs' Joke

Osama Hirota

王様 ↓

King Hirota

Dr. Fuchs' Joke

Osama Hirota

王様

King Hirota

Disciples of Hirota

Prof. Hirota's speech in QOC'90

Quantum Aspects of Optical Communications 1990

(Full version) 

Prof. Hirota's speech in QOC'90

Quantum Aspects of Optical Communications 1990

..... So far, the background of optical communications have been discussed independently in many scientific figure as mathematics, information theory, physics, and communication engineering. As a result, many symposiums were already held in each field. And an excellent progress in the general theory has been reported.
Unfortunately, there are still problems in understanding the fruitful results of scientific articles, because of a difference in various points of view, importance, and terminology. Now the interconnection of old fields should be required. And the exchange between scientists is necessary. Based on these considerations, this workshop was planned.

We believe that this is the first workshop which enables researchers in such a different fields to discuss on the quantum aspects of optical communications at a same place and a same time. .....

(Full version)

Prof. Hirota's speech in QOC'90

Quantum Aspects of Optical Communications 1990

(Full version) 

Dr. Fuchs' Joke

Osama Hirota

王様 ↓

King Hirota

Disciples of Hirota

Prof. Hirota's speech in QOC'90

Quantum Aspects of Optical Communications 1990

….. So far, the background of optical communications have been discussed independently in many scientific figure as mathematics, information theory, physics, and communication engineering. As a result, many symposiums were already held in each field. And an excellent progress in the general theory has been reported.
Unfortunately, there are still problems in understanding the fruitful results of scientific articles, because of a difference in various points of view, importance, and terminology. Now the interconnection of old fields should be required. And the exchange between scientists is necessary. Based on these considerations, this workshop was planned.

We believe that this is the first workshop which enables researchers in such a different fields to discuss on the quantum aspects of optical communications at a same place and a same time. …..

(Full version)

Approach from communication engineering

Channel coding theorem

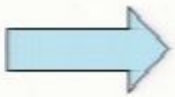
[Hausladen, Jozsa, Schumacher, Westmoreland, Wootters, PRA, 1996]

[Schumacher & Westmoreland, PRA, 1997]

[Holevo, IEEE IT, 1998]

& the above result imply

Modulation ?	continuous
Coding ?	random
Decoding ?	SRM(square-root meas.) on typical subspace



Difficult to realize
(even for the classical communications)

Approach from communication engineering

Channel coding theorem

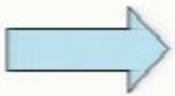
[Hausladen, Jozsa, Schumacher, Westmoreland, Wootters, PRA, 1996]

[Schumacher & Westmoreland, PRA, 1997]

[Holevo, IEEE IT, 1998]

& the above result imply

Modulation ?	continuous
Coding ?	random
Decoding ?	SRM(square-root meas.) on typical subspace



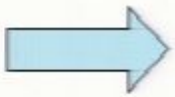
Difficult to realize
(even for the classical communications)

Approach from communication engineering

We consider

Modulation	discrete (digital)
Coding	linear code or pseudo-cyclic code
Decoding	SRM on code space

Modulation ?	continuous
Coding ?	random
Decoding ?	SRM(square-root meas.) on typical subspace



Difficult to realize
(even for the classical communications)

Purpose

To answer the following questions.

- Can capacity with discrete-valued input achieve the full capacity (capacity of continuous channel) ?

- What is the best quantum collective decoding for a certain class of codes ?

- What is the performance of the codes ?

- How to implement the quantum decoding or quantum receiver ?

Outline

[I] Capacity of attenuated channel with discrete-valued input.

Can capacity with discrete-valued input attain the full capacity ?

[II] Coding/decoding for discrete coherent-state signals

What is the best quantum collective decoding for a certain class of codes ?

What is the performance of the codes ?

How to implement the quantum decoding or quantum receiver ?

→ It will be talked elsewhere.

[I] Capacity of attenuated channel with discrete-valued input.

We consider an attenuated single mode optical channel when the energy (or average photon number) of the input signals is constrained.

Energy constraint: $\textit{average photon number} \leq N_S$

Transmissivity of an attenuated channel : η

[I] Capacity of attenuated channel with discrete-valued input.

We consider an attenuated single mode optical channel when the energy (or average photon number) of the input signals is constrained.

Energy constraint: $\textit{average photon number} \le N_S$

Transmissivity of an attenuated channel : η

Capacity of an attenuated channel:

$$C_{\text{full}} = g(\eta N_S)$$
$$g(x) = (x+1)\log(x+1) - x\log x$$

[Giovannetti et al., PRL, 2004]

[I] Capacity of attenuated channel with discrete-valued input.

Known Result:

Using coherent-state signals, Gaussian modulation, random coding, and SRM on typical subspace, the full capacity C_{full} is asymptotically achieved !

The full capacity was also compared with Heterodyne or Homodyne capacity in Ref.1 in order to estimate how well can we approach the capacity using conventional decoding procedure.

Ref.1:
Giovannetti, Guha, Lloyd, Maccone, Shapiro, Yuen,
"Classical Capacity of the Lossy Bosonic Channel: The Exact Solution,"
PRL92, (2004)

[I] Capacity of attenuated channel with discrete-valued input.

Homodyne and Heterodyne capacities:

Using coherent-state signals, Gaussian modulation, random coding, Homodyne or Heterodyne detection, and soft decoding,

$$C_{\text{hom}} = \frac{1}{2}\log_2\left(1+4\eta N_S\right)\text{[bits/letter]}$$

$$C_{\text{het}} = \log_2\left(1+\eta N_S\right)\text{[bits/letter]}$$

The above capacities are obtained by the formula :

$$C_{\text{Shannon}} = \frac{1}{2}\log_2\left(1+SNR\right)\text{[bits/letter]}$$

$$= W\log_2\left(1+SNR\right)\text{[bits/sec]}$$

[Shannon, 1948]

where W : bandwidth

[I] Capacity of attenuated channel with discrete-valued input.

Homodyne and Heterodyne capacities:

Using coherent-state signals, Gaussian modulation, random coding, Homodyne or Heterodyne detection, and soft decoding,

$$C_{\text{hom}} = \frac{1}{2}\log_2\left(1+4\eta N_S\right)\text{[bits/letter]}$$

$$C_{\text{het}} = \log_2\left(1+\eta N_S\right)\text{[bits/letter]}$$

Birth year of Hirota

The above capacities are obtained by the formula :

$$C_{\text{Shannon}} = \frac{1}{2}\log_2\left(1+SNR\right)\text{[bits/letter]}$$

$$= W\log_2\left(1+SNR\right)\text{[bits/sec]}$$

[Shannon, 1948]

where W : bandwidth

[I] Capacity of attenuated channel with discrete-valued input.

Homodyne and Heterodyne capacities:

Using coherent-state signals, Gaussian modulation, random coding, Homodyne or Heterodyne detection, and soft decoding,

$$C_{\text{hom}} = \frac{1}{2}\log_2\left(1+4\eta N_S\right)\text{[bits/letter]}$$

$$C_{\text{het}} = \log_2\left(1+\eta N_S\right)\text{[bits/letter]}$$

Heterodyne is asymptotically achieved the full capacity when $N_S \to \infty$

[I] Capacity of attenuated channel with discrete-valued input.

Homodyne and Heterodyne capacities:

Using coherent-state signals, Gaussian modulation, random coding, Homodyne or Heterodyne detection, and soft decoding,

$$C_{\text{hom}} = \frac{1}{2}\log_2\left(1+4\eta N_S\right)\ [\text{bits/letter}]$$

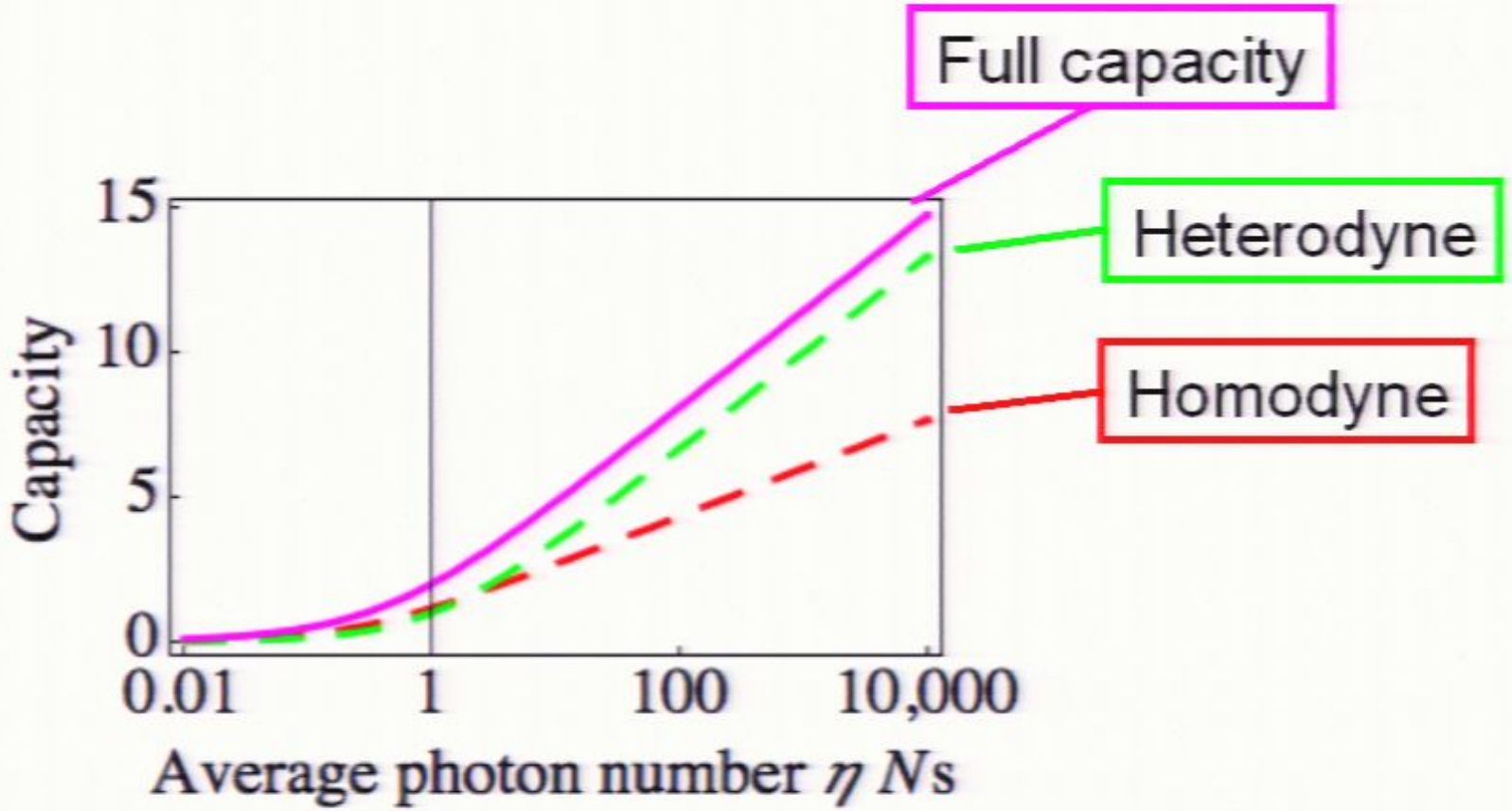
$$C_{\text{het}} = \log_2\left(1+\eta N_S\right)\ [\text{bits/letter}]$$

Heterodyne is asymptotically achieved the full capacity when $N_S \to \infty$

Q. How many photons are required to almost achieve the full capacity ?

[I] Capacity of attenuated channel with discrete-valued input.

Capacity of attenuated channel with continuous-valued input.



$$C_{\text{het}} / C_{\text{full}} \geq 0.90 \quad \text{when} \quad \eta N_S \geq 10{,}000$$

$$C_{\text{het}} / C_{\text{full}} \geq 0.95 \quad \text{when} \quad \eta N_S \geq 200{,}000{,}000$$

[I] Capacity of attenuated channel with discrete-valued input.

Capacity attained by digital modulation:

How many signals are required ?

I_M : Mutual information conveyed by M-ary signals

$$I_M \le \log_2 M [\text{bits}]$$

$$\Downarrow$$

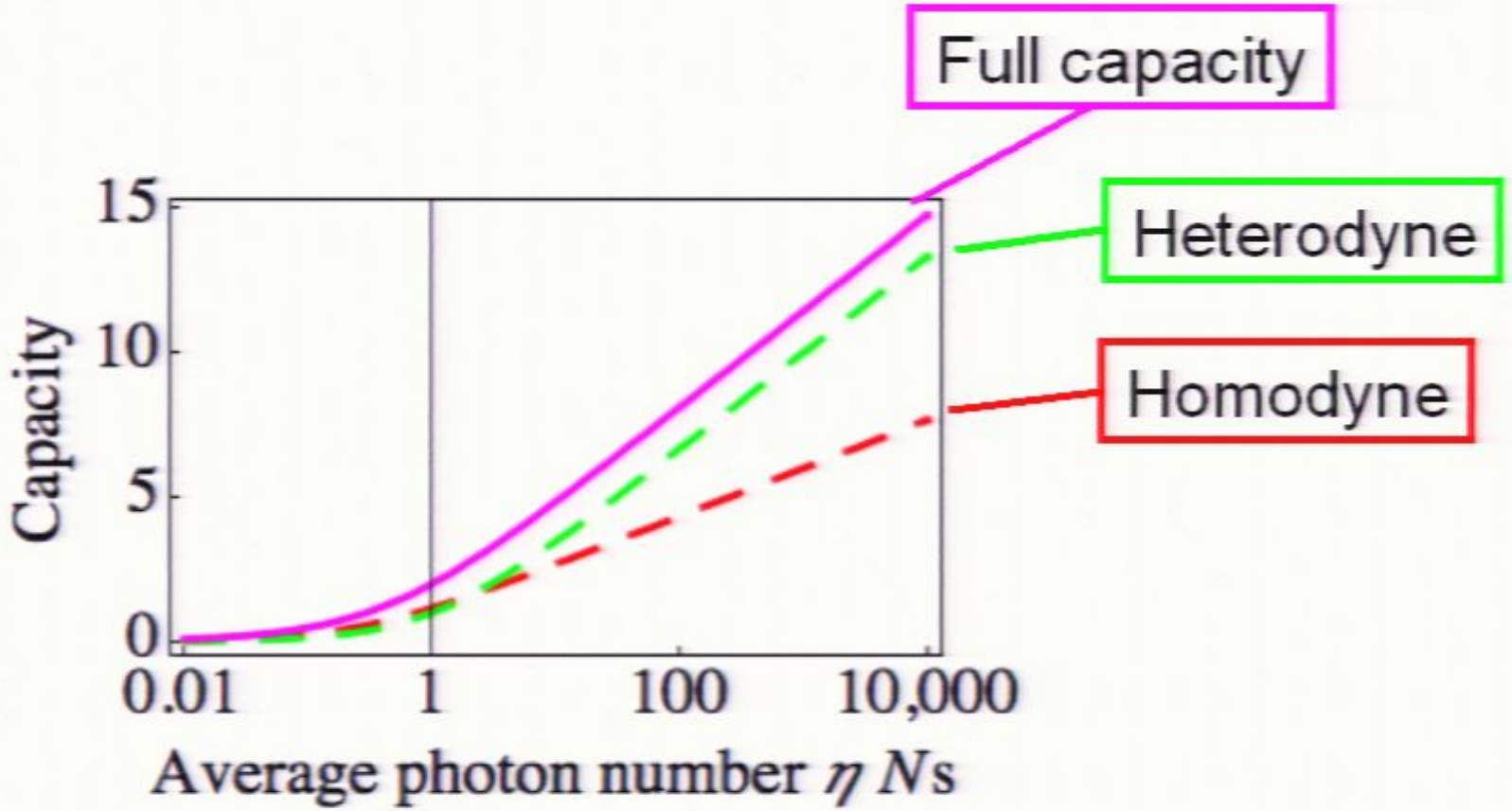
$$M \ge 2^{I_M}$$

So, the number of signals to almost achieve the capacity C must be satisfied

$$M \ge 2^C$$

[I] Capacity of attenuated channel with discrete-valued input.

Capacity of attenuated channel with continuous-valued input.



$$C_{\text{het}} / C_{\text{full}} \geq 0.90 \quad \text{when} \quad \eta N_S \geq 10{,}000$$

$$C_{\text{het}} / C_{\text{full}} \geq 0.95 \quad \text{when} \quad \eta N_S \geq 200{,}000{,}000$$

[I] Capacity of attenuated channel with discrete-valued input.

Homodyne and Heterodyne capacities:

Using coherent-state signals, Gaussian modulation, random coding, Homodyne or Heterodyne detection, and soft decoding,

$$C_{\text{hom}} = \frac{1}{2}\log_2\left(1+4\eta N_S\right)\ [\text{bits/letter}]$$

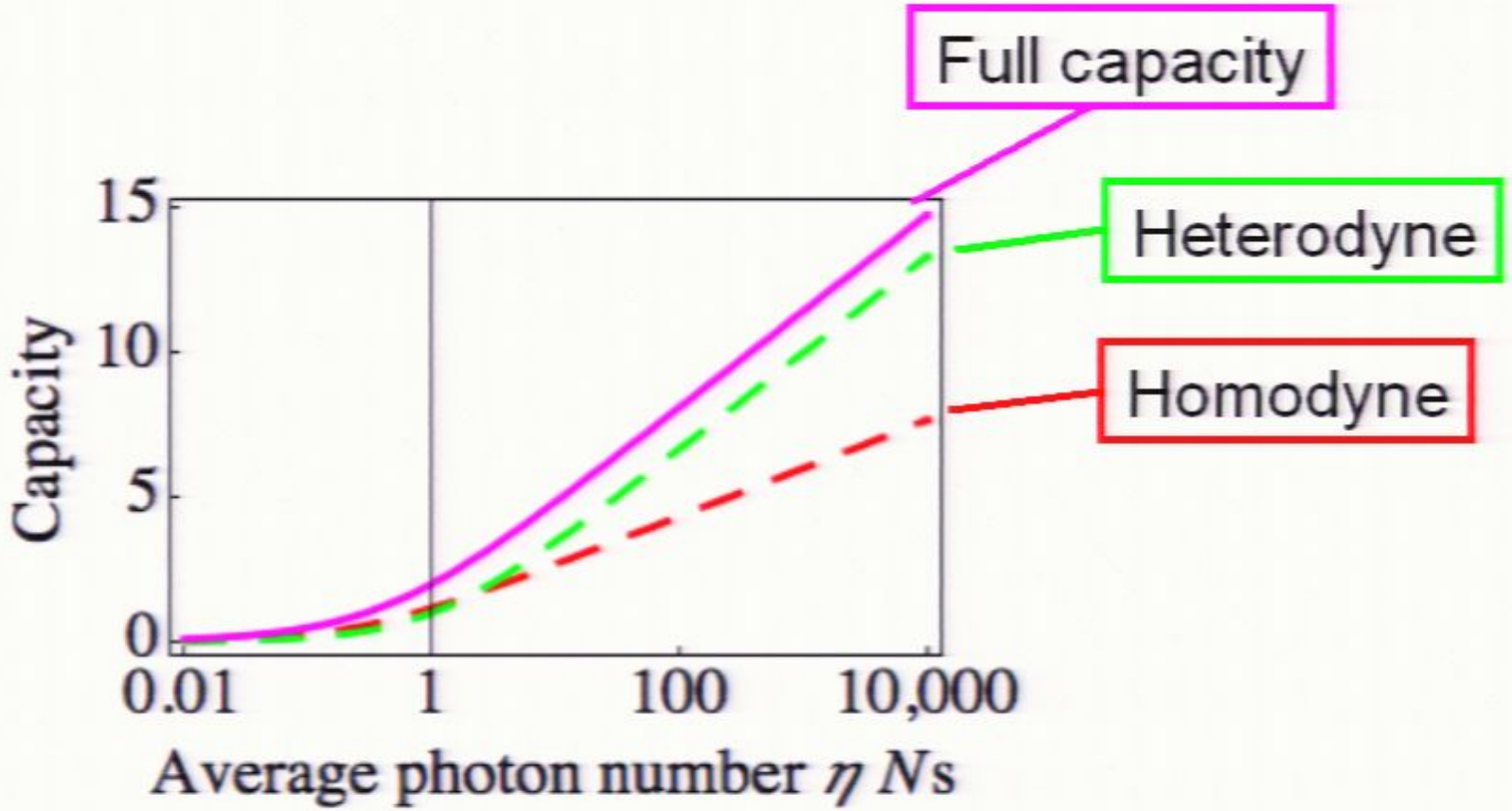
$$C_{\text{het}} = \log_2\left(1+\eta N_S\right)\ [\text{bits/letter}]$$

Heterodyne is asymptotically achieved the full capacity when $N_S \to \infty$

Q. How many photons are required to almost achieve the full capacity ?

[I] Capacity of attenuated channel with discrete-valued input.

Capacity of attenuated channel with continuous-valued input.



$$C_{\text{het}} / C_{\text{full}} \geq 0.90 \quad \text{when} \quad \eta N_S \geq 10{,}000$$

$$C_{\text{het}} / C_{\text{full}} \geq 0.95 \quad \text{when} \quad \eta N_S \geq 200{,}000{,}000$$

[I] Capacity of attenuated channel with discrete-valued input.

Capacity attained by digital modulation:

How many signals are required ?

I_M : Mutual information conveyed by M-ary signals

$$I_M \le \log_2 M [\text{bits}]$$

$$\Downarrow$$

$$M \ge 2^{I_M}$$

So, the number of signals to almost achieve the capacity C must be satisfied

$$M \ge 2^C$$

[I] Capacity of attenuated channel with discrete-valued input.

Capacity attained by digital modulation:

For the full capacity $C_{\text{full}} = (N+1)\log(N+1) - N\log N$

$$M \geq 2^{C_{\text{full}}} = (N+1)^{N+1} \cdot N^{-N} = (1+\frac{1}{N})^{1+N} \cdot N \qquad \text{detail}$$

$$\geq \mathrm{e} \cdot N \approx 2.718 \times N \qquad \geq \mathrm{e}$$

where $N = \eta N_S$ heterodyne

Ex. $N = 1$ $M \geq (1+1)^{1+1} \cdot 1^{-1} = 4$

$N = 10$ $M > 28$

$N = 10{,}000$ $M > 27{,}182$

[I] Capacity of attenuated channel with discrete-valued input.

In this research,

We consider PSK ($M > 2$) and QAM coherent-state signals.

PSK and QAM are usual digital modulations in conventional wireless communication systems.

Coherent-states attain the full capacity and are also robust.

[I] Capacity of attenuated channel with discrete-valued input.

In this research,

We consider PSK ($M > 2$) and QAM coherent-state signals.

PSK and QAM are usual digital modulations in conventional wireless communication systems.

Coherent-states attain the full capacity and are also robust.

Most related result:

Sohma & Hirota,
"Binary discretization for quantum continuous channels,"
PRA**62**, (2000)

The full capacity is almost achieved by BPSK signals when the energy of the signals is very small.

[I] Capacity of attenuated channel with discrete-valued input.

In this research,

We consider PSK ($M > 2$) and QAM coherent-state signals.

PSK and QAM are usual digital modulations in conventional wireless communication systems.

Coherent-states attain the full capacity and are also robust.

Most related result:

Sohma & Hirota,
"Binary discretization for quantum continuous channels,"
PRA**62**, (2000)

The full capacity is almost achieved by BPSK signals when the energy of the signals is very small.

⇒ We consider the case of three or more signals.

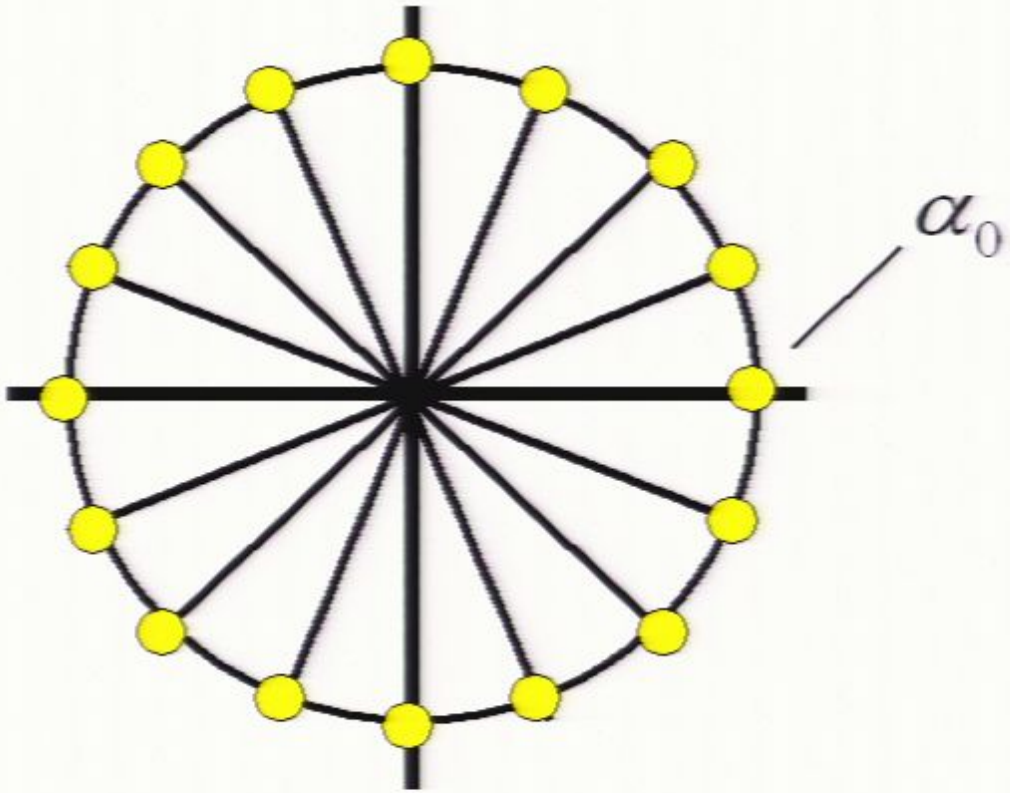
[I] Capacity of attenuated channel with discrete-valued input.

M-ary PSK coherent-state signals

PSK (Phase-shift keying) is a digital modulation scheme that conveys data by modulating the phase of a carrier wave.

$$|\alpha_k\rangle = \left|\alpha_0 \exp\left[\mathrm{i}\frac{2k}{M}\pi\right]\right\rangle$$

$$k = 0, \cdots, M-1$$



16PSK signals on phase plane

[I] Capacity of attenuated channel with discrete-valued input.

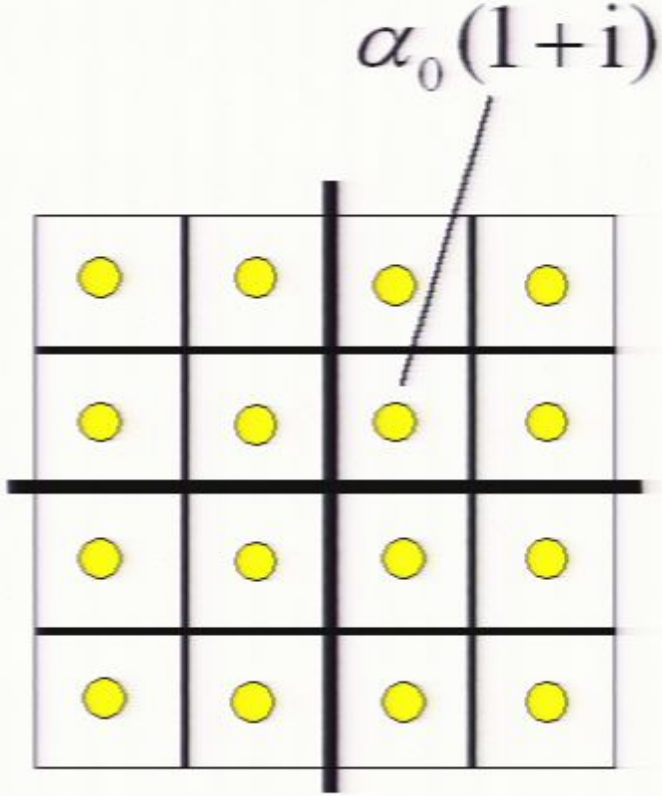
M-ary QAM coherent-state signals

QAM (Quadrature amplitude modulation) is a digital modulation scheme which conveys data by modulating the amplitude of two carrier waves.

$$\left|\alpha_{pq}\right\rangle = \left|\alpha_0\left(p+\mathrm{i}q\right)\right\rangle, \quad p,q \in \Omega$$

$$\Omega = \left\{-\left(L-1\right)+2\left(l-1\right) \middle| l = 1,2,\cdots,L\right\}$$

$$M = L^2$$



16QAM signals on phase plane

$$L = 4$$

$$\Omega = \{-3,-1,1,3\}$$

[I] Capacity of attenuated channel with discrete-valued input.

Capacity of attenuated channel with discrete-valued input

The capacity of an attenuated channel when coherent state signals are used as discrete-valued input is

$$C = \max_{\xi_i, \alpha_0} \left\{ S\left(\sum_{i=0}^{M-1} \xi_i \rho_i^{(\text{out})} \right) - \sum_{i=0}^{M-1} \xi_i S\left(\rho_i^{(\text{out})} \right) \right\} = \max_{\xi_i, \alpha_0} \left\{ S\left(\sum_{i=0}^{M-1} \xi_i \rho_i^{(\text{out})} \right) \right\}$$

where ξ_i : *a priori* probability $S(\bullet)$: von Neumann entropy

$\rho_i^{(\text{in})} = |\alpha_i\rangle\langle\alpha_i|$: input coherent-state

$\rho_i^{(\text{out})} = |\sqrt{\eta}\alpha_i\rangle\langle\sqrt{\eta}\alpha_i|$: attenuated signal

and the maximization is performed under the constraint :

$$\sum_{i=0}^{M-1} \xi_i |\alpha_i|^2 \le N_S$$

[I] Capacity of attenuated channel with discrete-valued input.

Maximization of von Neumann entropy under energy constraint

(1) Case of PSK signals:

$$\sum_{i=0}^{M-1}\xi_i|\alpha_i|^2 = \sum_{i=0}^{M-1}\xi_i|\alpha_0|^2 = |\alpha_0|^2\sum_{i=0}^{M-1}\xi_i = |\alpha_0|^2 \le N_S$$

$$\Longrightarrow \quad |\alpha_0|^2 = N_S$$

It is sufficient to optimize *a priori* probabilities.

[I] Capacity of attenuated channel with discrete-valued input.

Maximization of von Neumann entropy under energy constraint

(1) Case of PSK signals:

$$\sum_{i=0}^{M-1}\xi_i|\alpha_i|^2=\sum_{i=0}^{M-1}\xi_i|\alpha_0|^2=|\alpha_0|^2\sum_{i=0}^{M-1}\xi_i=|\alpha_0|^2\le N_S$$

$$\Longrightarrow \quad |\alpha_0|^2=N_S$$

It is sufficient to optimize *a priori* probabilities.

Theorem

$$\xi_i=1/M\ (\forall i)$$

Uniform distribution is optimum.

[Kato, Osaki, Hirota, PLA**245**, 1999]

[I] Capacity of attenuated channel with discrete-valued input.

Maximization of von Neumann entropy under energy constraint

(2) Case of QAM signals:

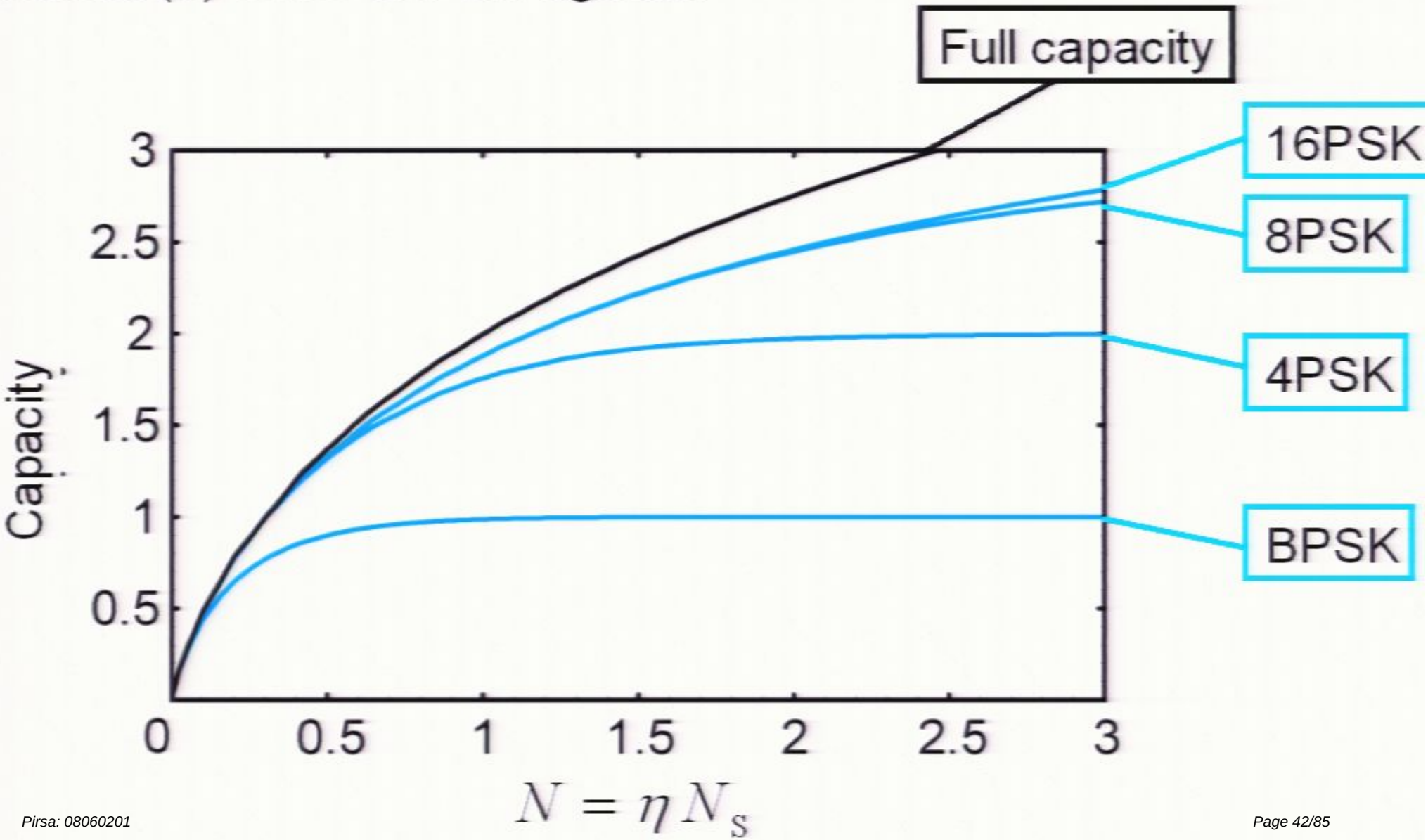
Both *a priori* probabilities and coherent amplitude should be optimized.

And QAM signals are not symmetric signals.

Numerical optimization is necessary.

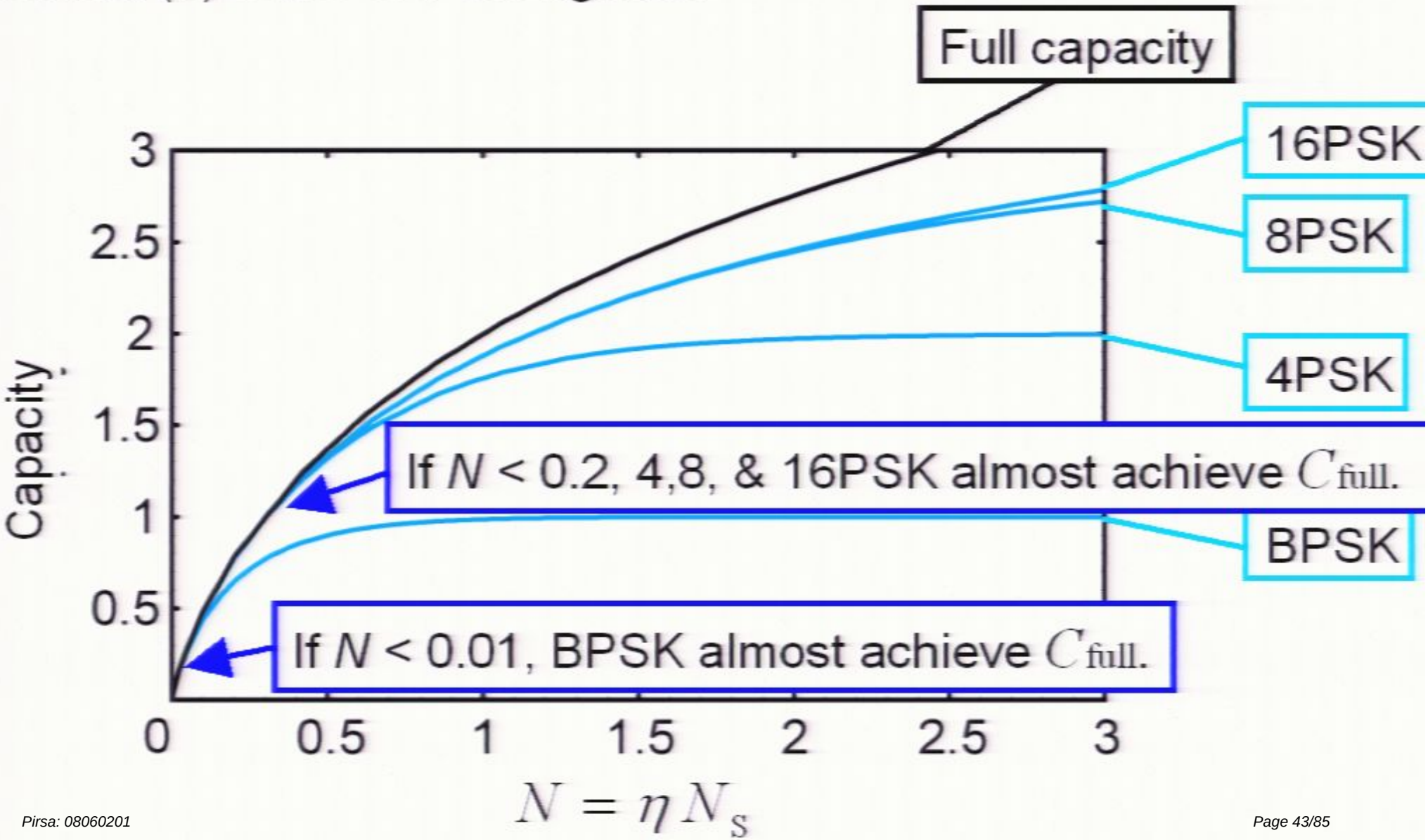
[I] Capacity of attenuated channel with discrete-valued input.

Result (1) Case of PSK signals:



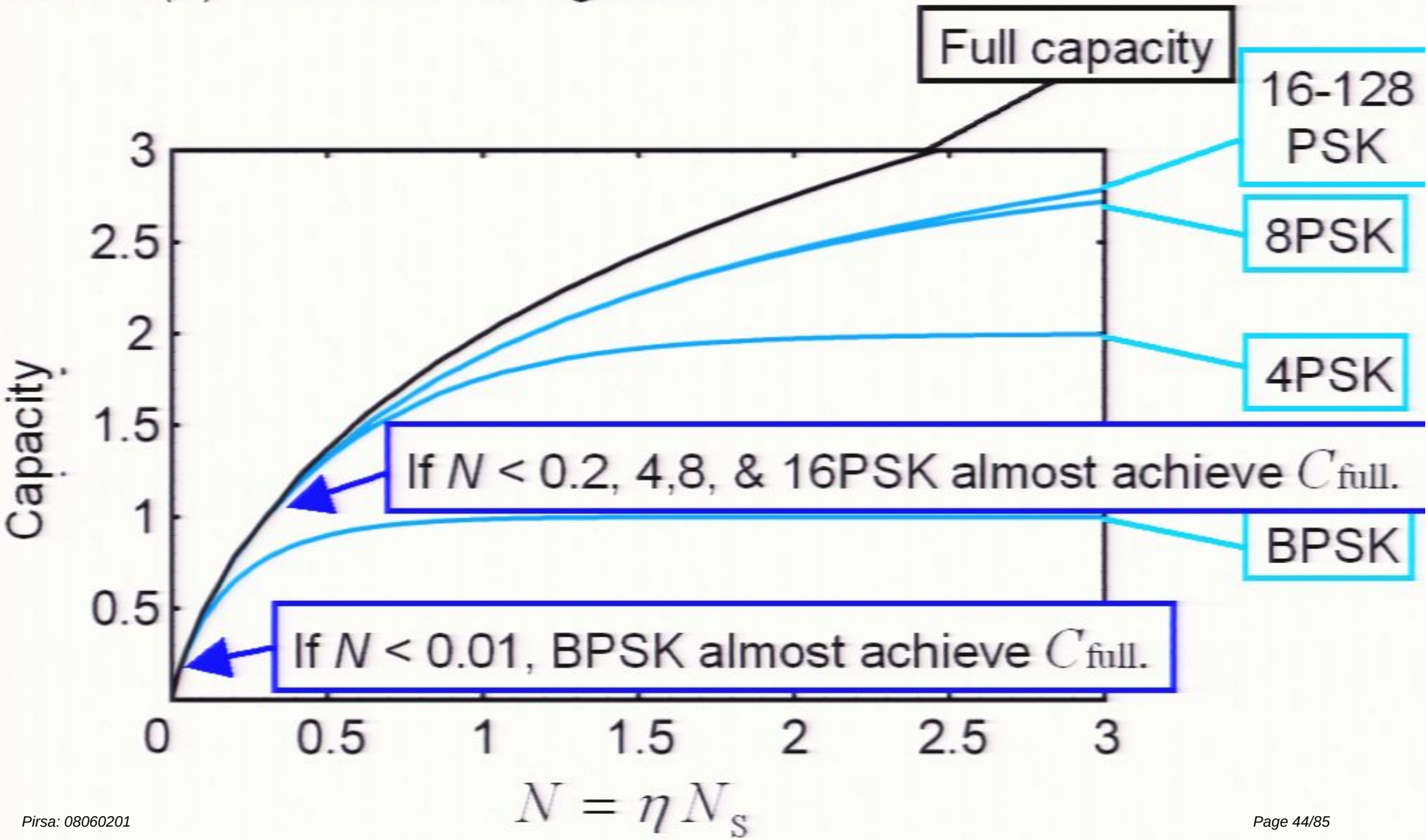
[I] Capacity of attenuated channel with discrete-valued input.

Result (1) Case of PSK signals:



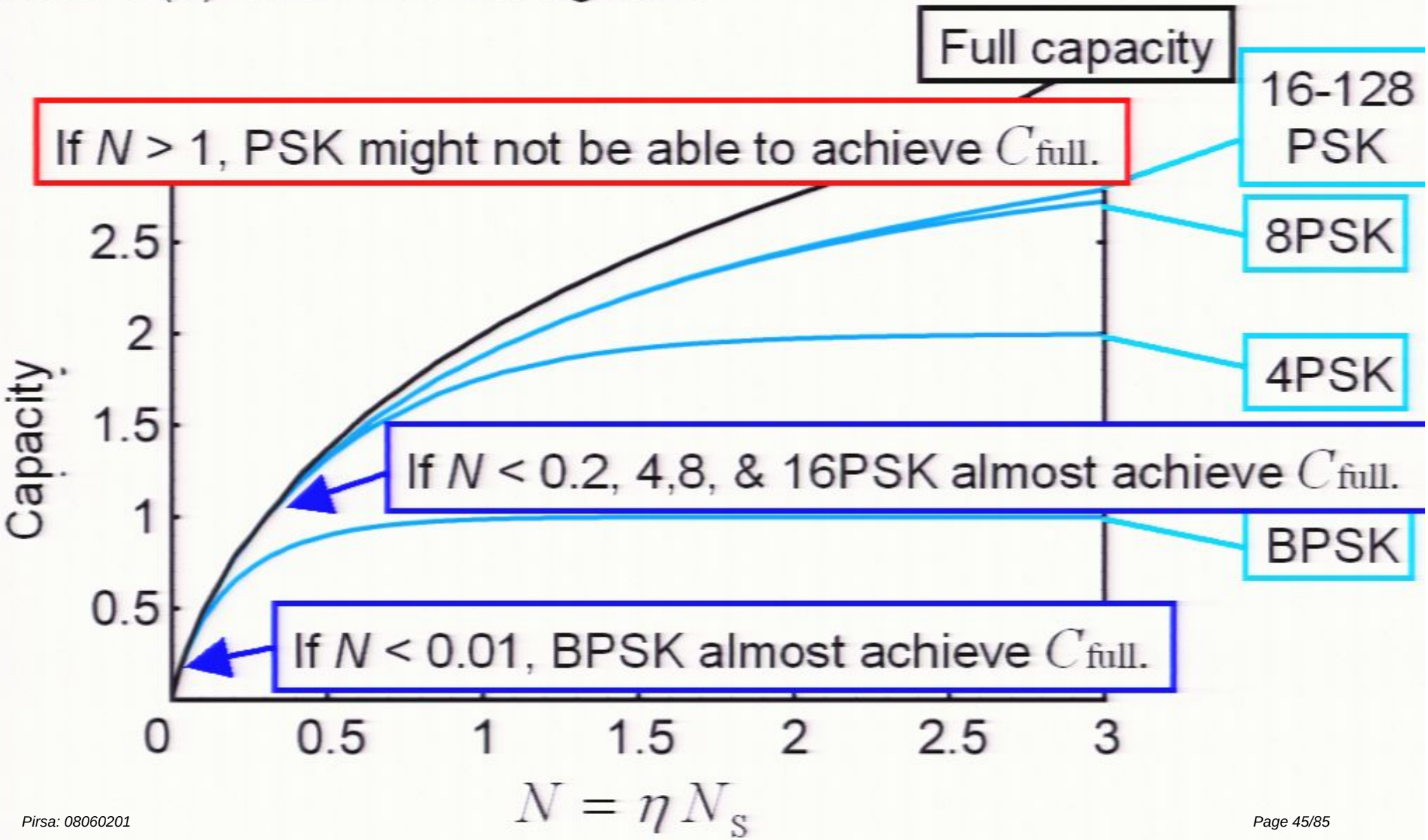
[I] Capacity of attenuated channel with discrete-valued input.

Result (1) Case of PSK signals:



[I] Capacity of attenuated channel with discrete-valued input.

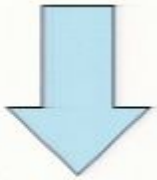
Result (1) Case of PSK signals:



[I] Capacity of attenuated channel with discrete-valued input.

Result (1) Case of PSK signals:

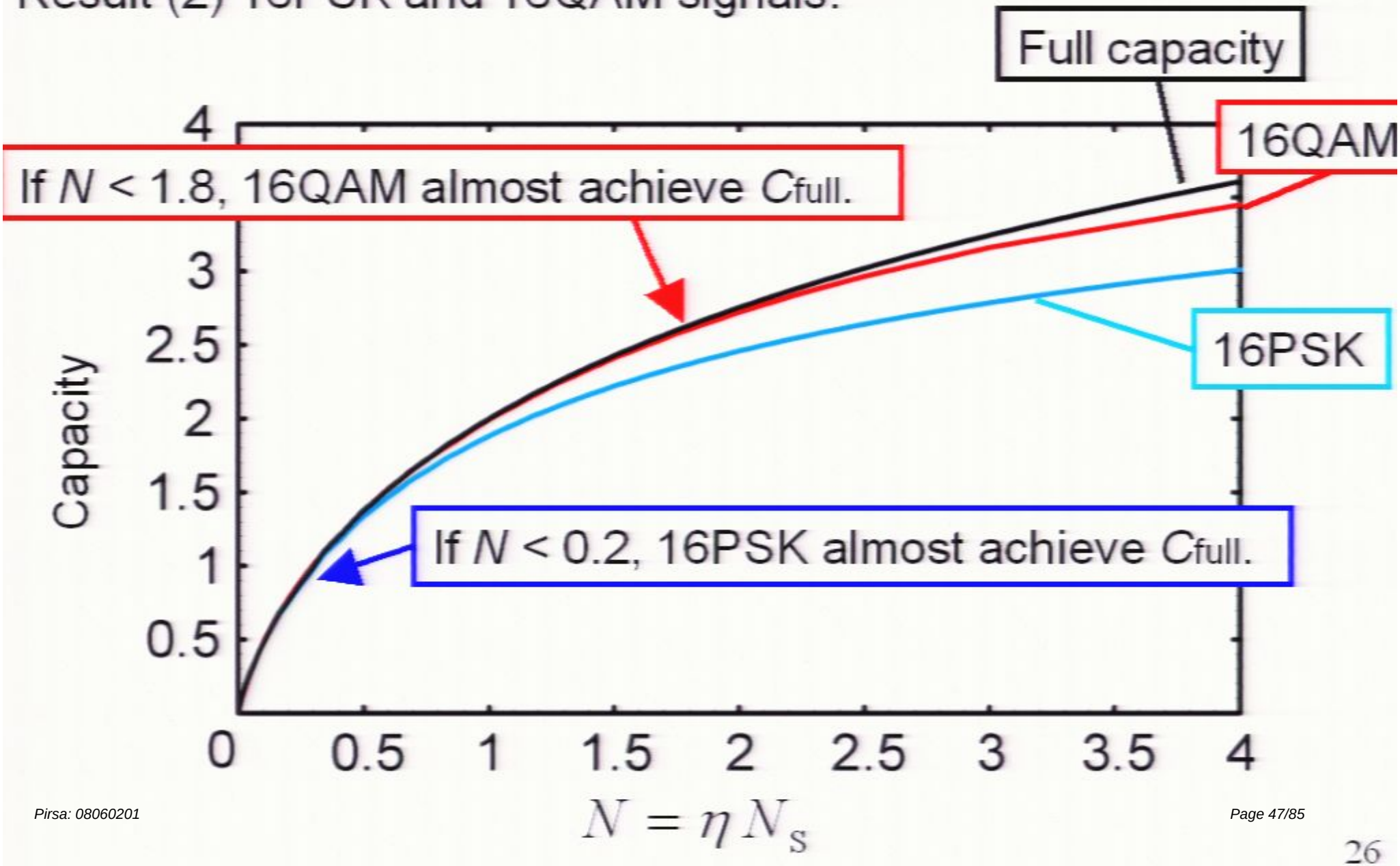
If $N > 1$, PSK might not be able to achieve C_{full}.



For N > 1, we must modulate not only phase but also amplitude.

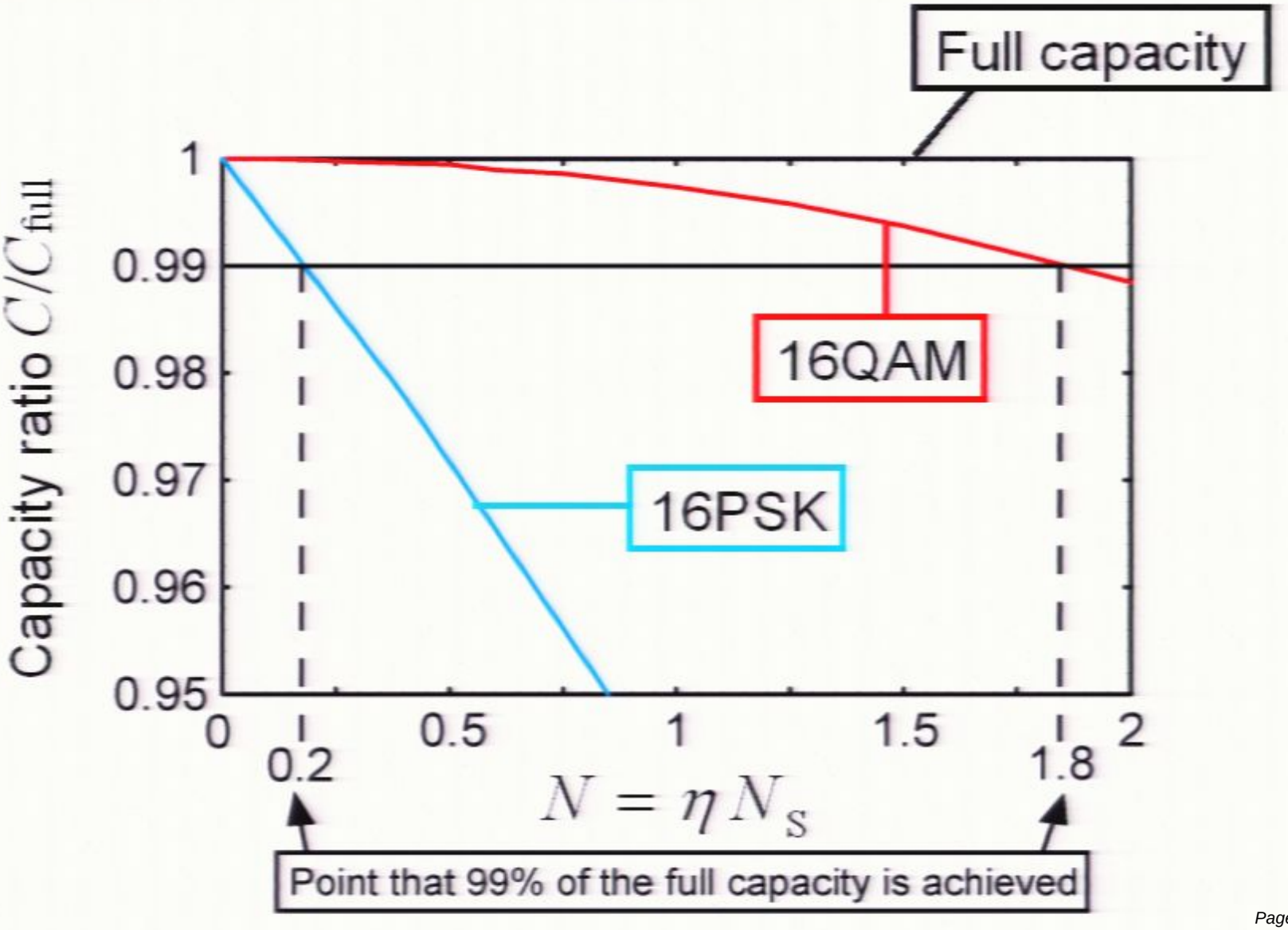
[I] Capacity of attenuated channel with discrete-valued input.

Result (2) 16PSK and 16QAM signals:



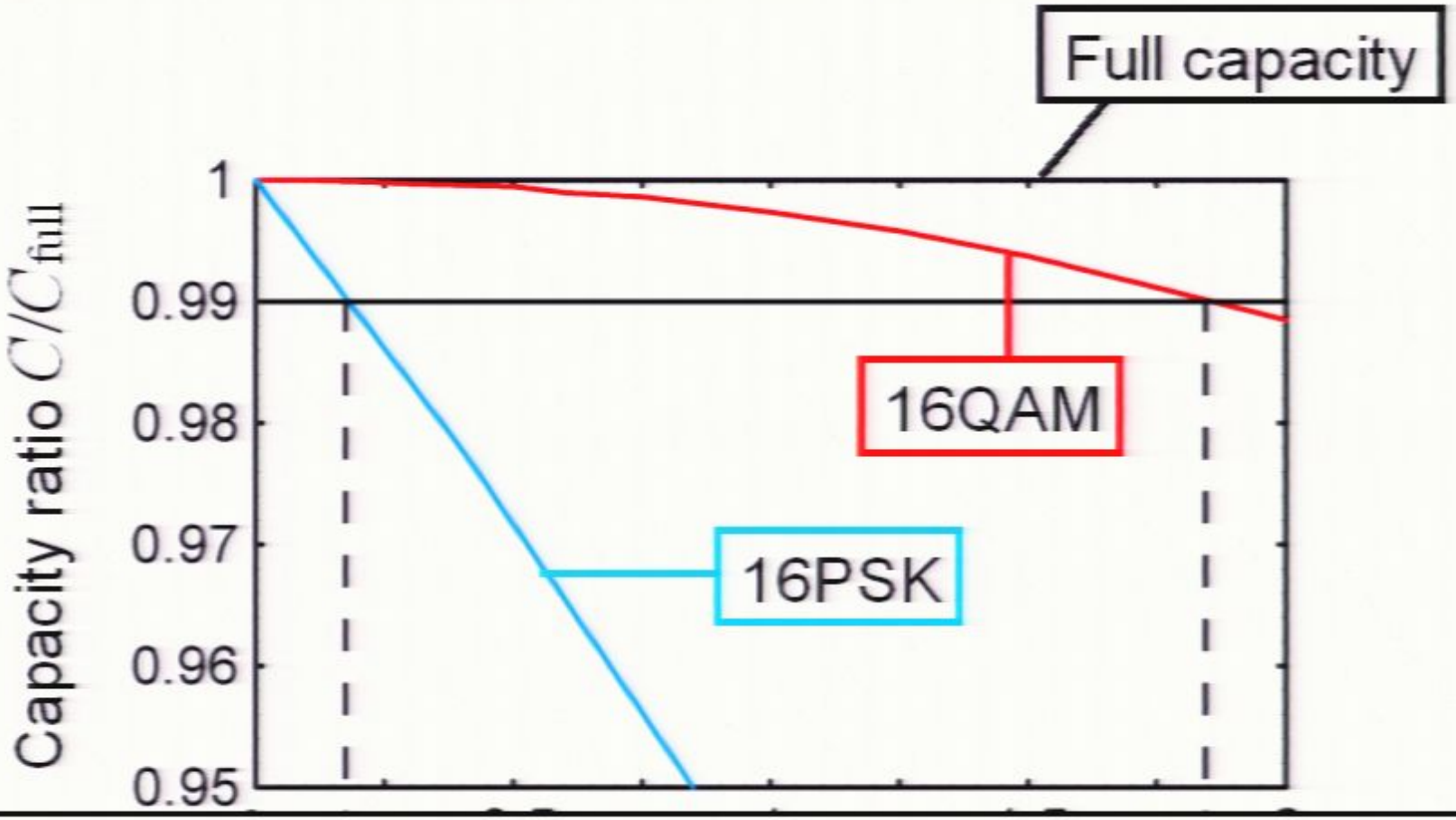
[I] Capacity of attenuated channel with discrete-valued input.

Comparison of 16PSK with 16QAM signals:



[I] Capacity of attenuated channel with discrete-valued input.

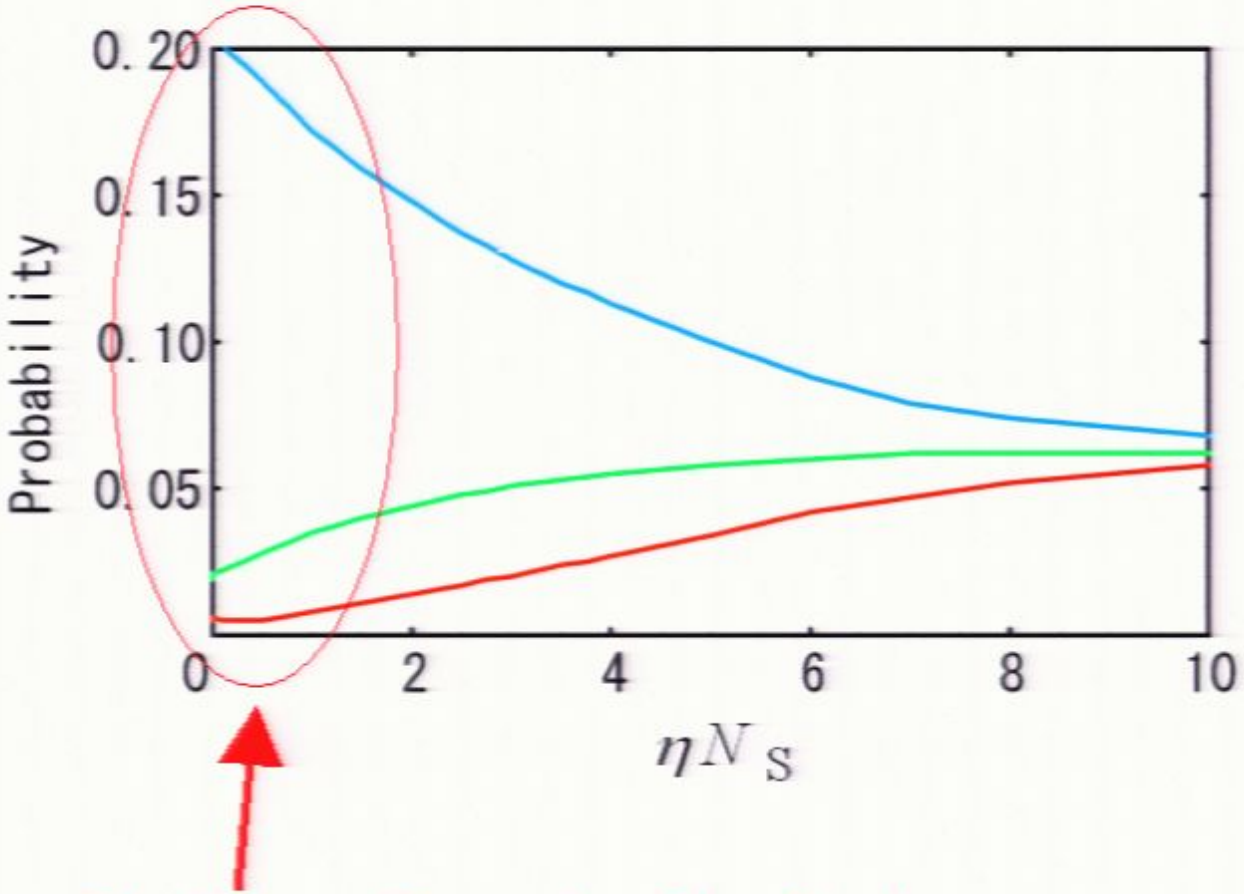
Comparison of 16PSK with 16QAM signals:



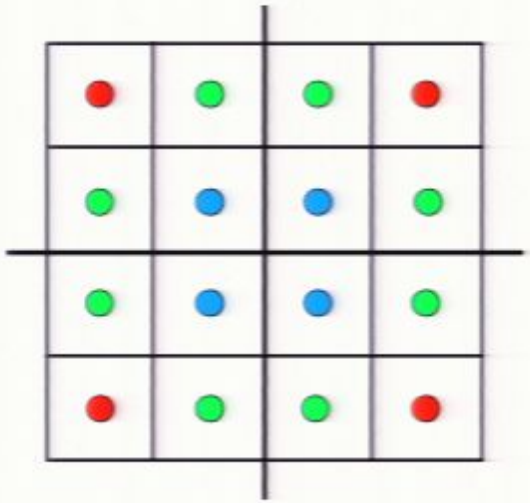
The range of signal energy, in which the full capacity is almost achieved becomes 9 times wider by changing the modulation.

[I] Capacity of attenuated channel with discrete-valued input.

Probability distribution by which the capacity with 16QAM is attained:



Similar to Gaussian distribution



16QAM signals on phase plane

Conclusion [I]

Can capacity with discrete-valued input attain the full capacity ?

[I] Capacity of attenuated channel with discrete-valued input.

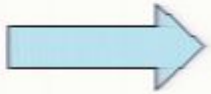
Conclusion [I]

Can capacity with discrete-valued input attain the full capacity ?

⇒ Yes !

Conclusion [I]

Can capacity with discrete-valued input attain the full capacity ?



Yes !

When N <1.8, the full capacity is almost achieved by 16QAM.

Appropriate QAM may achieve the full capacity.

[II] Coding/decoding for discrete coherent-state signals

What is the best quantum collective decoding for a certain class of codes ?

What is the performance of the codes ?

(How to implement the quantum decoding or quantum receiver ?)

Relation between topics [I] and [II]

Topic [I] : Capacity

Topic [II] : Coding/Decoding

[II] Coding/decoding for discrete coherent-state signals

What is the best quantum collective decoding for a certain class of codes ?

What is the performance of the codes ?

(How to implement the quantum decoding or quantum receiver ?)

Relation between topics [I] and [II]

Topic [I] : Capacity	Asymptotic	Ultimate limit
⬇	⬇	⬇
Topic [II] : Coding/Decoding	Finite	Realizable

[II] Coding/decoding for discrete coherent-state signals

What is the best quantum (collective) decoding for a certain class of codes ?

to minimize the average probability of error

Find quantum decoding $\{\Pi_j\}$

to minimize $P_{\mathrm{e}}\left(\{\zeta_i\},\{\hat{w}_i\},\{\Pi_j\}\right)=1-\sum_{i=0}^{|\mathbf{C}|-1}\zeta_i \mathrm{Tr}\,\hat{w}_i\Pi_i$

where ζ_i : *a priori* probability of the codeword w_i

$\hat{w}_i$: (received) codeword-state corresponding to w_i

$w_i\,(\in\mathbf{C})$: (classical) codeword, $\mathbf{C}$: (classical) code

$\{\Pi_j\}$: quantum decoding (POVM on $\mathrm{supp}\{\hat{w}_i\}$)

[II] Coding/decoding for discrete coherent-state signals

What is the best quantum (collective) decoding for a certain class of codes ?

to minimize the average probability of error

Find quantum decoding $\{\Pi_j\}$

to minimize $P_{\mathrm{e}}\left(\{\zeta_i\},\{\hat{w}_i\},\{\Pi_j\}\right)=1-\sum_{i=0}^{|\mathbf{C}|-1}\zeta_i \mathrm{Tr}\,\hat{w}_i\Pi_i$

$1/|\mathbf{C}|$ (we assume uniform distribution)

where ζ_i : *a priori* probability of the codeword w_i

$\hat{w}_i$: (received) codeword-state corresponding to w_i

$w_i\,(\in\mathbf{C})$: (classical) codeword, $\mathbf{C}$: (classical) code

$\{\Pi_j\}$: quantum decoding (POVM on $\mathrm{supp}\{\hat{w}_i\}$)

[II] Coding/decoding for discrete coherent-state signals

What is the best quantum collective decoding for a certain class of codes ?

(1) Binary codes

Proposition

SRM is optimum to minimize the average probability of error for any binary linear code when the signals are pure.

[Sasaki, Kato, Izutsu, Hirota, PRA, 1998]
[Usuda, Takumi, Hata, Hirota, PLA, 1999]

(2) M-ary codes

Proposition

SRM is optimum to minimize the average probability of error for any M-ary pseudo-cyclic code when the signals are symmetric pure states.

[Eldar & Forney, PRA, 2001]
[Usuda, Usami, Takumi, Hata, PLA, 2002]

(2) M-ary codes

Proposition

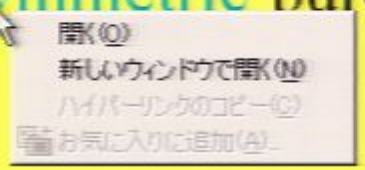
SRM is optimum to minimize the average probability of error for any M-ary pseudo-cyclic code when the signals are SVI[illegible] states.

[Eldar & Forney, PRA, 2001]
[Usuda, Usami, Takumi, Hata, PLA, 2002]

(2) M-ary codes

Proposition

SRM is optimum to minimize the average probability of error for any M-ary pseudo-cyclic code when the signals are symmetric pure states.



[Eldar & Forney, PRA, 2001]
[Usuda, Usami, Takumi, Hata, PLA, 2002]

(2) M-ary codes

Proposition

SRM is optimum to minimize the average probability of error for any M-ary pseudo-cyclic code when the signals are symmetric pure states.

[Eldar & Forney, PRA, 2001]
[Usuda, Usami, Takumi, Hata, PLA, 2002]

Symmetric signals

Definition : Symmetric signals

Let $\{\rho_i \,|\, i = 0,1,\ldots,M-1\}$ be a set of quantum signal states

$\{\rho_i\}$ is called ***symmetric***

if there exists a unitary operator U

such that $\rho_i = U^i \rho_0 (U^i)^{\mathrm{T}}, \quad \forall i$

where T : Hermite conjugate

Case of pure states

$\{|\psi_i\rangle \,|\, i = 0,1,\ldots,M-1\}$ is symmetric if $|\psi_i\rangle = U^i |\psi_0\rangle, \forall i$

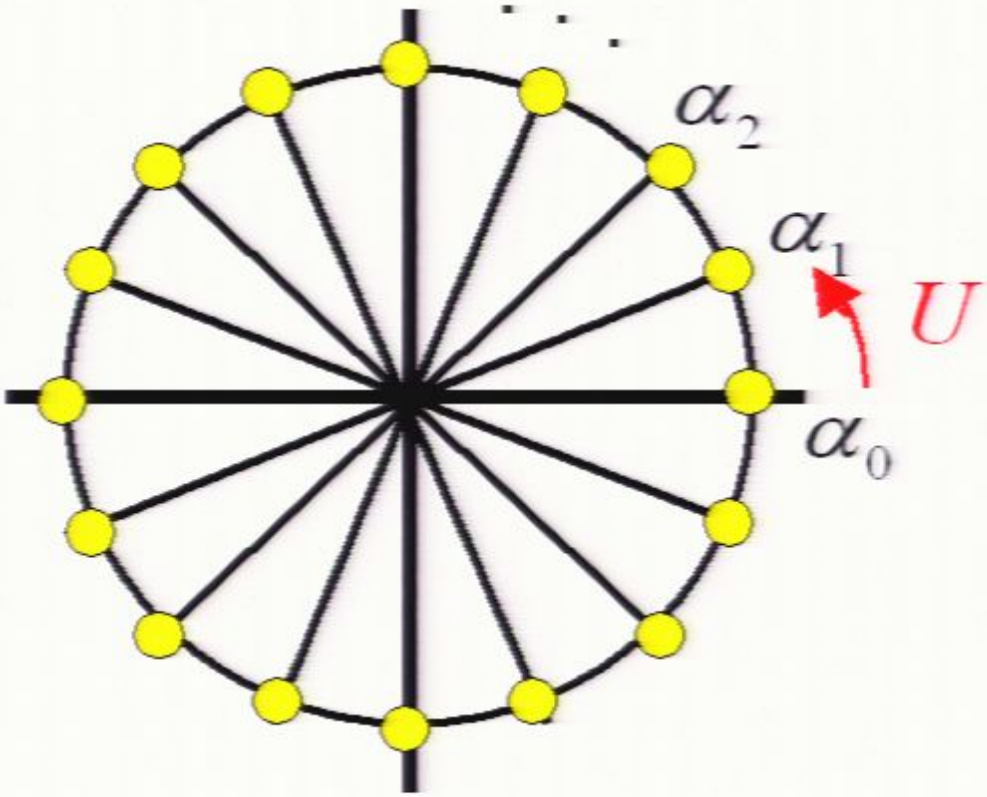
Symmetric signals (ex. PSK signals)

$$|\alpha_k\rangle = \left|\alpha_0 \exp\left[\mathrm{i}\frac{2k}{M}\pi\right]\right\rangle$$

$$k = 0, \cdots, M-1$$

$$|\alpha_k\rangle = U^k |\alpha_0\rangle$$

$$U = \exp\left[\mathrm{i}\frac{2\pi}{M} a^T a\right]$$



16PSK signals
on phase plane

Case of pure states

$\{|\psi_i\rangle | i = 0,1,\ldots,M-1\}$ is symmetric if $|\psi_i\rangle = U^i |\psi_0\rangle, \forall i$

(2) M-ary codes

Proposition

SRM is optimum to minimize the average probability of error for any M-ary pseudo-cyclic code when the signals are symmetric pure states.

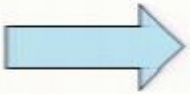
[Eldar & Forney, PRA, 2001]
[Usuda, Usami, Takumi, Hata, PLA, 2002]

(2) M-ary codes

Proposition

SRM is optimum to minimize the average probability of error for any M-ary pseudo-cyclic code when the signals are symmetric pure states.

[Eldar & Forney, PRA, 2001]
[Usuda, Usami, Takumi, Hata, PLA, 2002]



The best quantum collective decoding for PSK coherent-state signals coded by pseudo-cyclic codes is the SRM.

(2) M-ary codes

Proposition

SRM is optimum to minimize the average probability of error for any M-ary pseudo-cyclic code when the signals are symmetric pure states.

[Eldar & Forney, PRA, 2001]
[Usuda, Usami, Takumi, Hata, PLA, 2002]

The best quantum collective decoding for PSK coherent-state signals coded by pseudo-cyclic codes is the SRM.

For coded QAM signals, the best decoding is unknown.

What is the performance of the codes ?

Definition : Square-root measurement (SRM)

For M-ary pure-state signals $\{|\psi_i\rangle | i = 0,\ldots,M-1\}$

the SRM is defined as $\{\Pi_j = |\mu_j\rangle\langle\mu_j| \,|\, j = 0,\ldots,M-1\}$

where $|\mu_j\rangle = \Phi^{-1/2}|\psi_j\rangle$ and is called a measurement state

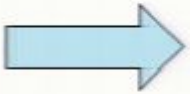
and $\Phi = \sum_{i=0}^{M-1} |\psi_i\rangle\langle\psi_i|$

(2) M-ary codes

Proposition

SRM is optimum to minimize the average probability of error for any M-ary pseudo-cyclic code when the signals are symmetric pure states.

[Eldar & Forney, PRA, 2001]
[Usuda, Usami, Takumi, Hata, PLA, 2002]



The best quantum collective decoding for PSK coherent-state signals coded by pseudo-cyclic codes is the SRM.

For coded QAM signals, the best decoding is unknown.

[II] Coding/decoding for discrete coherent-state signals

What is the performance of the codes ?

Definition : Square-root measurement (SRM)

For M-ary pure-state signals $\{|\psi_i\rangle | i = 0,\ldots,M-1\}$

the SRM is defined as $\{\Pi_j = |\mu_j\rangle\langle\mu_j| \,|\, j = 0,\ldots,M-1\}$

where $|\mu_j\rangle = \Phi^{-1/2}|\psi_j\rangle$ and is called a measurement state

and $\Phi = \sum_{i=0}^{M-1} |\psi_i\rangle\langle\psi_i|$

[II] Coding/decoding for discrete coherent-state signals

What is the performance of the codes ?

In order to evaluate performance of coding/decoding, we can use the following lemma.

Lemma

For M-ary pure-state signals $\{|\psi_i\rangle | i = 0,\ldots,M-1\}$

$$\langle \mu_j | \psi_i \rangle = \left(\Gamma^{1/2}\right)_{i,j}$$

where $|\mu_j\rangle$ is a measurement state of the SRM

and $\Gamma = \left[\langle \psi_i | \psi_j \rangle\right]$ is the Gram matrix.

[Hausladen, Jozsa, Schumacher, Westmoreland, Wootters, PRA, 1996]

[II] Coding/decoding for discrete coherent-state signals

This lemma is useful not only for the proof of the channel coding theorem but also for computing some quantities when the codeword length is finite.

Lemma

For M-ary pure-state signals $\{|\psi_i\rangle | i = 0,\ldots,M-1\}$

$$\langle \mu_j | \psi_i \rangle = \left(\Gamma^{1/2}\right)_{i,j}$$

where $|\mu_j\rangle$ is a measurement state of the SRM

and $\Gamma = \left[\langle \psi_i | \psi_j \rangle\right]$ is the Gram matrix.

[Hausladen, Jozsa, Schumacher, Westmoreland, Wootters, PRA, 1996]

[II] Coding/decoding for discrete coherent-state signals

This lemma is useful not only for the proof of the channel coding theorem but also for computing some quantities when the codeword length is finite.

Problem: To compute the square-root of the Gram matrix is hard when the number of codewords is large (more than 1,000).

[II] Coding/decoding for discrete coherent-state signals

This lemma is useful not only for the proof of the channel coding theorem but also for computing some quantities when the codeword length is finite.

Problem: To compute the square-root of the Gram matrix is hard when the number of codewords is large (more than 1,000).

We have tried to simplify the calculation.

[II] Coding/decoding for discrete coherent-state signals

(1) Binary codes

Proposition

For any binary linear (n, k) code $\mathbf{C} = \{w_i | i = 0, \ldots, 2^k - 1\}$ the (i, j) component of the square-root of Gram matrix is calculated as

$$\left(\Gamma^{1/2}\right)_{i,j} = \left(\Gamma^{1/2}\right)_{0, i \oplus j}$$

$$\left(\Gamma^{1/2}\right)_{0,j} = \frac{1}{2^k} \sum_{m=0}^{2^k-1} (-1)^{w_{\mathrm{H}}(j \cdot m)} \sqrt{\sum_{l=0}^{2^k-1} (-1)^{w_{\mathrm{H}}(m \cdot l)} \Gamma_{0,l}}$$

where $\Gamma = \left[\left\langle w_i \middle| w_j \right\rangle\right]$ is the Gram matrix.

[Usami, Usuda, Takumi, Hata, IEICE Trans., 1999]

[II] Coding/decoding for discrete coherent-state signals

(2) q-ary codes

Proposition

For any q-ary pseudo-cyclic (n, k) code $\mathbf{C} = \{w_i | i = 0, \ldots, q^k - 1\}$ the (i, j) component of the square-root of Gram matrix is calculated as

$$\left(\Gamma^{1/2}\right)_{i,j} = \left(\Gamma^{1/2}\right)_{0,i+j^{-1}}$$

$$\left(\Gamma^{1/2}\right)_{0,j} = \frac{1}{q^k} \sum_{m=0}^{q^k-1} \alpha^{\langle j,m \rangle} \sqrt{\sum_{l=0}^{q^k-1} \alpha^{\langle m,l \rangle} \Gamma_{0,l}}$$

if q is a prime number and the letter-states are symmetric and pure.
where $\alpha = \exp[2\pi i/q]$.

[Usuda, Usami, Takumi, Hata, PLA, 2002]

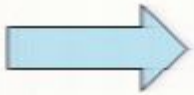
[II] Coding/decoding for discrete coherent-state signals

(3) M-ary codes

Proposition

The proposition is further generalized to any group covariant M-ary code.
Here $M = 2, 3, 4, 5, 6, \ldots$

[Shiromoto, Usuda, in preparation]



We can apply the formula to BPSK, 3PSK, 4PSK, ….

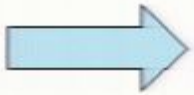
[II] Coding/decoding for discrete coherent-state signals

(3) M-ary codes

Proposition

The proposition is further generalized to any group covariant M-ary code.
Here $M = 2, 3, 4, 5, 6, \ldots$

[Shiromoto, Usuda, in preparation]



We can apply the formula to BPSK, 3PSK, 4PSK, ….

To apply this formula to concrete modulations and codings is in progress.

Conclusion [II]

What is the best quantum collective decoding for a certain class of codes ?

How can we evaluate efficiently the performance ?

Conclusion [II]

What is the best quantum collective decoding for a certain class of codes ?

The SRM is the best decoding to minimize average probability of error for any pseudo-cyclic code when the letter-states are symmetric and pure.

How can we evaluate efficiently the performance ?

Conclusion [II]

What is the best quantum collective decoding for a certain class of codes ?

→ The SRM is the best decoding to minimize average probability of error for any pseudo-cyclic code when the letter-states are symmetric and pure.

How can we evaluate efficiently the performance ?

→ We can use the formula of channel matrix for any group covariant code.

Conclusion [II]

What is the best quantum collective decoding for a certain class of codes ?

→ The SRM is the best decoding to minimize average probability of error for any pseudo-cyclic code when the letter-states are symmetric and pure.

How can we evaluate efficiently the performance ?

→ We can use the formula of channel matrix for any group covariant code.

Remaining problem:

Optimum decoding and its formula for coded QAM signals (non-symmetric signals).

Summary

The ultimate capacity is certainly important but I'm interested in how to use the result and how to connect with technology.

Summary

The ultimate capacity is certainly important but I'm interested in how to use the result and how to connect with technology.

Although the result of our study is neither scientific nor sensational, I think such a study is necessary to realize "fast, reliable, and secure optical quantum communications" in near future.

Conclusion [II]

What is the best quantum collective decoding for a certain class of codes ?

→ The SRM is the best decoding to minimize average probability of error for any pseudo-cyclic code when the letter-states are symmetric and pure.

How can we evaluate efficiently the performance ?

→ We can use the formula of channel matrix for any group covariant code.

Remaining problem:

Optimum decoding and its formula for coded QAM signals (non-symmetric signals).