
OPTICAL COMMUNICATION THEORY AND TECHNIQUES

Edited by

ENRICO FORESTIERI
Scuola Superiore Sant'Anna, Pisa, Italy

 Springer

Contents

Preface	ix
Part I Information and Communication Theory for Optical Communications	
Solving the Nonlinear Schrödinger Equation <i>Enrico Forestieri and Marco Secondini</i>	3
Modulation and Detection Techniques for DWDM Systems <i>Joseph M. Kahn and Keang-Po Ho</i>	13
Best Optical Filtering for Duobinary Transmission <i>G. Bosco, A. Carena, V. Curri, and P. Poggiolini</i>	21
Theoretical Limits for the Dispersion Limited Optical Channel <i>Roberto Gaudino</i>	29
Capacity Bounds for MIMO Poisson Channels with Inter-Symbol Interference <i>Alfonso Martinez</i>	37
Qspace Project: Quantum Cryptography in Space <i>C. Barbieri, G. Cariolaro, T. Occhipinti, C. Pernechele, F. Tamburini, P. Villoresi</i>	45
Quantum-Aided Classical Cryptography with a Moving Target <i>Fabrizio Tamburini, Sante Andreoli, and Tommaso Occhipinti</i>	53
Part II Coding Theory and Techniques	
Channel Coding for Optical Communications <i>Sergio Benedetto and Gabriella Bosco</i>	63
Soft Decoding in Optical Systems: Turbo Product Codes vs. LDPC Codes <i>Gabriella Bosco and Sergio Benedetto</i>	79
Iterative Decoding and Error Code Correction Method in Holographic Data Storage <i>Attila Sütő and Emőke Lőrincz</i>	87

Performance of Optical Time-Spread CDMA/PPM with Multiple Access and Multipath Interference <i>B. Zeidler, G. C. Papen, and L. Milstein</i>	95
Performance Analysis and Comparison of Trellis-Coded and Turbo-Coded Optical CDMA Systems <i>M. Kulkarni, P. Purohit, and N. Kannan</i>	103
Part III Characterizing, Measuring, and Calculating Performance in Optical Fiber Communication Systems	
A Methodology For Calculating Performance in an Optical Fiber Communications System <i>C. R. Menyuk, B. S. Marks, and J. Zweck</i>	113
Markov Chain Monte Carlo Technique for Outage Probability Evaluation in PMD-Compensated Systems <i>Marco Secondini, Enrico Forestieri, and Giancarlo Prati</i>	121
A Parametric Gain Approach to Performance Evaluation of DPSK/DQPSK Systems with Nonlinear Phase Noise <i>P. Serena, A. Orlandini, and A. Bononi</i>	129
Characterization of Intrachannel Nonlinear Distortion in Ultra-High Bit-Rate Transmission Systems <i>Robert I. Killey, Vitaly Mikhailov, Shamil Appathurai, and Polina Bayvel</i>	137
Mathematical and Experimental Analysis of Interferometric Crosstalk Noise Incorporating Chirp Effect in Directly Modulated Systems <i>Efraim Buimovich-Rotem and Dan Sadot</i>	151
On the Impact of MPI in All-Raman Dispersion-Compensated IMDD and DPSK Links <i>Stefan Tenenbaum and Pierluigi Poggiolini</i>	157
Part IV Modulation Formats and Detection	
Modulation Formats for Optical Fiber Transmission <i>Klaus Petermann</i>	167
Dispersion Limitations in Optical Systems Using Offset DPSK <i>Jin Wang and Joseph M. Kahn</i>	173
Integrated Optical FIR-Filters for Adaptive Equalization of Fiber Channel Impairments at 40 Gbit/s <i>M. Bohn, W. Rosenkranz, F. Horst, B. J. Offrein, G.-L. Bona, P. Krummrich</i>	181
Performance of Electronic Equalization Applied to Innovative Transmission Techniques <i>Vittorio Curri, Roberto Gaudino, and Antonio Napoli</i>	189

<i>Contents</i>	vii
Performance Bounds of MLSE in Intensity Modulated Fiber Optic Links <i>N. Alić, G. C. Papen, L. B. Milstein, P. H. Siegel, and Y. Fainman</i>	197
On MLSE Reception of Chromatic Dispersion Tolerant Modulation Schemes <i>Helmut Griesser, Joerg-Peter Elbers, and Christoph Glingener</i>	205
Author Index	213
Index	215

Preface

Since the advent of optical communications, a great technological effort has been devoted to the exploitation of the huge bandwidth of optical fibers. Starting from a few Mb/s single channel systems, a fast and constant technological development has led to the actual 10 Gb/s per channel dense wavelength division multiplexing (DWDM) systems, with dozens of channels on a single fiber. Transmitters and receivers are now ready for 40 Gb/s, whereas hundreds of channels can be simultaneously amplified by optical amplifiers.

Nevertheless, despite such a pace in technological progress, optical communications are still in a primitive stage if compared, for instance, to radio communications: the widely spread on-off keying (OOK) modulation format is equivalent to the rough amplitude modulation (AM) format, whereas the DWDM technique is nothing more than the optical version of the frequency division multiplexing (FDM) technique. Moreover, adaptive equalization, channel coding or maximum likelihood detection are still considered something “exotic” in the optical world. This is mainly due to the favourable characteristics of the fiber optic channel (large bandwidth, low attenuation, channel stability, ...), which so far allowed us to use very simple transmission and detection techniques.

But now we are slightly moving toward the physical limits of the fiber and, as it was the case for radio communications, more sophisticated techniques will be needed to increase the spectral efficiency and counteract the transmission impairments. At the same time, the evolution of the *techniques* should be supported, or better preceded, by an analogous evolution of the *theory*. Looking at the literature, contradictions are not unlikely to be found among different theoretical works, and a lack of standards and common theoretical basis can be observed. As an example, the performance of an optical system is often given in terms of different, and sometimes misleading, figures of merit, such as the error probability, the Q-factor, the eye-opening and so on. Under very strict hypotheses, there is a sort of equivalence among these figures of merit, but things drastically change when nonlinear effects are present or different modulation formats considered.

This depiction of optical communications as an early science is well reflected by the most known journals and conferences of this area, where technological and experimental aspects usually play a predominant role. On the other hand, this book, namely *Optical Communications Theory and Techniques*, is intended to be a collection of up-to-date papers dealing with the theoretical aspects of optical communications. All the papers were selected or written by worldwide recognized experts in the field, and were presented at the 2004 Tyrrhenian International Workshop on Digital Communications. According to the program of the workshop, the book is divided into four parts:

Information and Communication Theory for Optical Communications. This first part examines optical systems from a rigorous information theory point of view, addressing questions like “what is the ultimate capacity of a given channel?”, or “which is the most efficient modulation format?”.

Coding Theory and Techniques. This part is concerned with the theory and techniques of coding, applied to optical systems. For instance, different forward error correction (FEC) codes are analyzed and compared, taking explicitly into account the non-AWGN (Additive White Gaussian Noise) nature of the channel.

Characterizing, Measuring, and Calculating Performance in Optical Fiber Communication Systems. This part describes several techniques for the experimental measurement, analytical evaluation or simulations-based estimation of the performance of optical systems. The error probability in the linear and nonlinear regime, as well as the impact of PMD or Raman amplification are subject of this part.

Modulation Formats and Detection. This last part is concerned with the joint or disjoint use of different modulation formats and detection techniques to improve the performance of optical systems and their tolerance to transmission impairments. Modulation in the amplitude, phase and polarization domain are considered, as well as adaptive equalization and maximum likelihood sequence estimation.

Each paper is self contained, such to give the reader a clear picture of the treated topic. Furthermore, getting back to the depiction of optical communications as an early science, the whole book is intended to be a common basis for the theoreticians working in the field, upon which consistent new works could be developed in the next future.

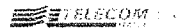
ENRICO FORESTIERI

Acknowledgments

The editor and general chair of the 2004 edition of the Tyrrhenian International Workshop on Digital Communications, held in Pisa on October 2004 as a topical meeting on "Optical Communication Theory and Techniques", is much indebted and wish to express his sincere thanks to the organizers of the technical sessions, namely *Joseph M. Kahn* from Stanford University, USA, *Sergio Benedetto* from Politecnico di Torino, Italy, *Curtis R. Menyuk* from University of Maryland Baltimore County, USA, and *Klaus Petermann* from Technische Universität Berlin, Germany, whose precious cooperation was essential to the organization of the Workshop.

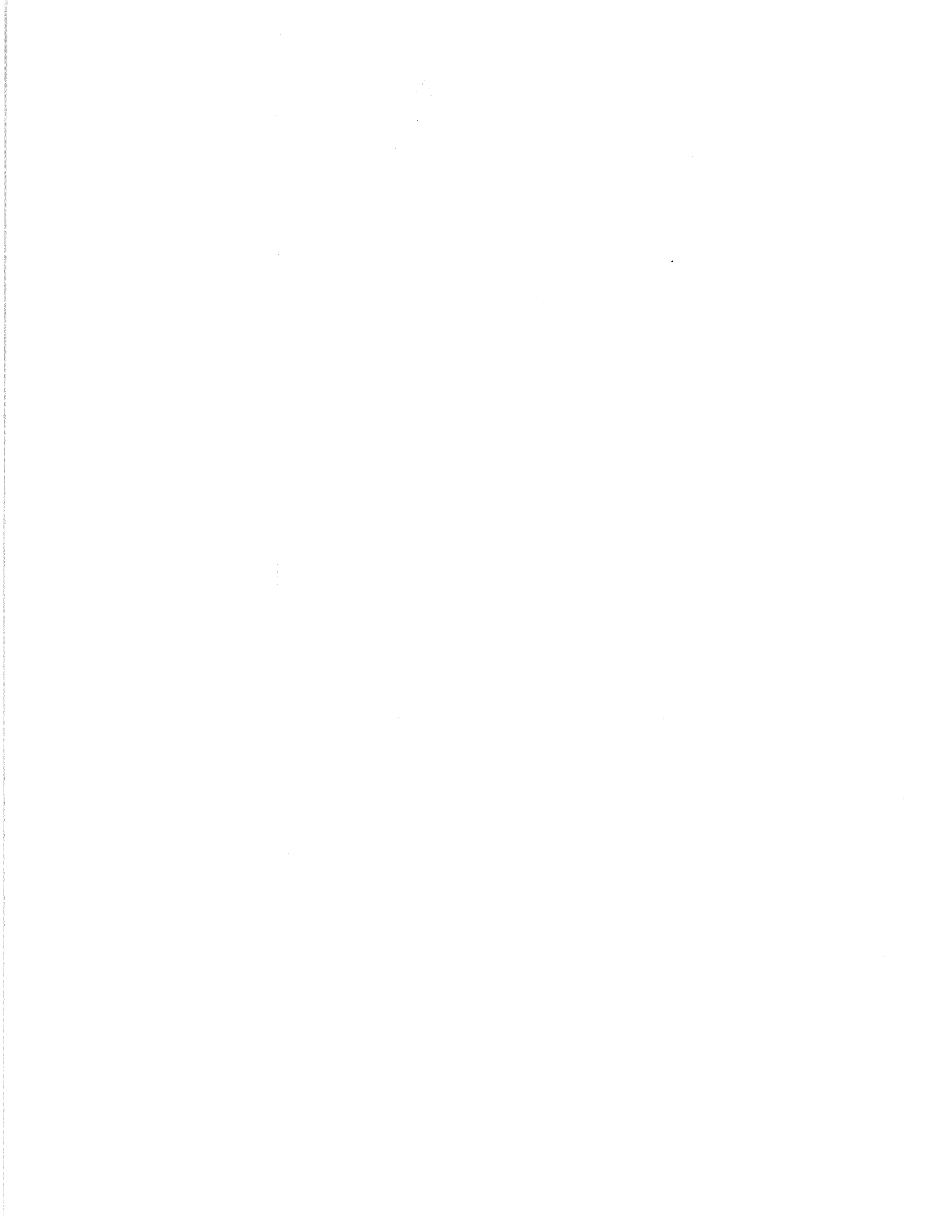
He would also like to thank all the authors for contributing to the Workshop with their high quality papers. Special thanks go to Giancarlo Prati, CNIT director, and to Marco Secondini and Karin Ennser, who generously helped in the preparation of this book.

The Workshop would not have been possible without the support of the Italian National Consortium for Telecommunications (CNIT), and without the sponsorship of the following companies, which are gratefully acknowledged.

The Marconi logo features the word "Marconi" in a stylized, cursive script font, with a horizontal line underneath the text.The Alcatel logo consists of the word "ALCATEL" in a bold, sans-serif font, with a horizontal line underneath the text.The Agilent Technologies logo features a stylized starburst icon to the left of the text "Agilent Technologies" in a bold, sans-serif font.The Siemens logo consists of the word "SIEMENS" in a bold, sans-serif font, with the tagline "Global network of innovation" in a smaller font below it.The Telecom logo features a stylized graphic of horizontal lines to the left of the word "TELECOM" in a bold, sans-serif font.The Anritsu logo consists of the word "Anritsu" in a bold, sans-serif font, with the tagline "Discover What's Possible™" in a smaller font below it.

I

INFORMATION AND COMMUNICATION
THEORY FOR OPTICAL COMMUNICATIONS



SOLVING THE NONLINEAR SCHRÖDINGER EQUATION

Enrico Forestieri and Marco Secondini

Scuola Superiore Sant'Anna di Studi Universitari e Perfezionamento, Pisa, Italy, and Photonic Networks National Laboratory, CNIT, Pisa, Italy.

forestieri@sssup.it

Abstract: Some simple recursive methods are described for constructing asymptotically exact solutions of the nonlinear Schrödinger equation (NLSE). It is shown that the NLSE solution can be expressed analytically by two recurrence relations corresponding to two different perturbation methods.

Key words: optical Kerr effect; optical fiber nonlinearity; nonlinear distortion; optical fiber theory.

1. INTRODUCTION

The nonlinear Schrödinger equation governs the propagation of the optical field complex envelope $v(z, t)$ in a single-mode fiber [1]. Accounting for group velocity dispersion (GVD), self-phase modulation (SPM), and loss, in a time frame moving with the signal group velocity, the NLSE can be written as

$$\frac{\partial v}{\partial z} = j \frac{\beta_2}{2} \frac{\partial^2 v}{\partial t^2} - j \gamma |v|^2 v - \frac{\alpha}{2} v, \quad (1)$$

where γ is the Kerr nonlinear coefficient [1], α is the power attenuation constant, and β_2 is the GVD parameter ($\beta_2 = -\lambda^2 D / (2\pi c)$, λ being the reference wavelength, c the light speed, and D the fiber dispersion parameter at λ). Letting $v(z, t) \triangleq e^{-\alpha z/2} u(z, t)$, we can get rid of the last term in (1), which becomes

$$\frac{\partial u}{\partial z} = j \frac{\beta_2}{2} \frac{\partial^2 u}{\partial t^2} - j \gamma e^{-\alpha z} |u|^2 u. \quad (2)$$

Exact solutions of this equation are typically not known in analytical form, except for soliton solutions when $\alpha = 0$ [2–4]. Given an input condition

$u(0, t)$, the solution of (2) is then to be found numerically, the most widely used method being the *Split-Step Fourier Method* (SSFM) [1]. Analytical approximations to the solution of (2) can be obtained by linearization techniques [5–12], such as perturbation methods tailored for modulation instability (or parametric gain) [5–8] or of more general validity [9, 10], small-signal analysis [11], and the variational method [12]. An approach based on Volterra series [13] was recently shown to be equivalent to the regular perturbation method [9]. However, all methods able to deal with an arbitrarily modulated input signal, provide accurate approximations either only for very small input powers or only for very small fiber losses, with the exception of the *enhanced* regular perturbation method presented in [9] and the multiplicative approximation introduced in [10], whose results are valid for input powers as high as about 10 dBm. We present here two recursive expressions that, starting from the linear solution of (2) for $\gamma = 0$, asymptotically converge to the exact solution for $\gamma \neq 0$, and revisit the multiplicative approximation in [10], relating it to the regular perturbation method.

2. AN INTEGRAL EXPRESSION OF THE NLSE

In this Section we will obtain an integral expression of the NLSE which, to our knowledge, is not found in the literature. Letting

$$f(z, t) \triangleq e^{-\alpha z} |u(z, t)|^2 u(z, t) \quad (3)$$

and taking the Fourier transform¹ of (2), we obtain

$$\frac{\partial U}{\partial z} = -j \frac{\beta_2}{2} \omega^2 U - j\gamma F, \quad (4)$$

which, by the position

$$U(z, \omega) \triangleq e^{-j\beta_2 \omega^2 z/2} Y(z, \omega), \quad (5)$$

becomes

$$\frac{\partial Y}{\partial z} = -j\gamma e^{j\beta_2 \omega^2 z/2} F. \quad (6)$$

Integrating (6) from 0 to z leads to

$$Y(z, \omega) = Y(0, \omega) - j\gamma \int_0^z e^{j\beta_2 \omega^2 \zeta/2} F(\zeta, \omega) d\zeta, \quad (7)$$

and, taking into account (5), we have

$$U(z, \omega) = U_0(z, \omega) - j\gamma \int_0^z e^{-j\beta_2 \omega^2 (z-\zeta)/2} F(\zeta, \omega) d\zeta, \quad (8)$$

¹The Fourier transform with respect to time t of a function $x(z, t)$ will be denoted by the same but capital letter $X(z, \omega)$, such that $X(z, \omega) = \mathcal{F}\{x(z, t)\}$, and $x(z, t) = \mathcal{F}^{-1}\{X(z, \omega)\}$.

where $U_0(z, \omega) = U(0, \omega)e^{-j\beta_2\omega^2 z/2}$ is the Fourier transform of the solution of (2) for $\gamma = 0$. Letting now $H(z, \omega) \triangleq \exp(-j\beta_2\omega^2 z/2)$, so that $h(z, t) = \mathcal{F}^{-1}\{H(z, \omega)\}$, and antitransforming (8) by taking into account (3), gives

$$u(z, t) = u_0(z, t) - j\gamma \int_0^z [|u(\zeta, t)|^2 u(\zeta, t)] \otimes h(z - \zeta, t) e^{-\alpha\zeta} d\zeta \quad (9)$$

where \otimes denotes temporal convolution, and $u_0(z, t) = u(0, t) \otimes h(z, t)$ is the signal at z in a linear and lossless fiber.

3. A FIRST RECURRENCE RELATION CORRESPONDING TO A REGULAR PERTURBATION METHOD

According to the regular perturbation (RP) method [9], expanding the optical field complex envelope $u(z, t)$ in power series in γ

$$u(z, t) = \sum_{k=0}^{\infty} \gamma^k u_k(z, t) \quad (10)$$

and substituting (10) in (9), after some algebra we obtain

$$\sum_{k=1}^{\infty} \gamma^k u_k = \sum_{n=0}^{\infty} \gamma^{n+1} \left[-j \int_0^z \left(\sum_{k=0}^n \sum_{i=0}^k u_i u_{k-i} u_{n-k}^* \right) \otimes h(z - \zeta, t) e^{-\alpha\zeta} d\zeta \right] \quad (11)$$

where we omitted the arguments (z, t) for the u_k 's appearing on the left side, and (ζ, t) for those on the right side. By equating the powers in γ with the same exponent, we can recursively evaluate all the u_k 's

$$u_n = -j \int_0^z \left(\sum_{k=0}^{n-1} \sum_{i=0}^k u_i u_{k-i} u_{n-k}^* \right) \otimes h(z - \zeta, t) e^{-\alpha\zeta} d\zeta, \quad n \geq 1. \quad (12)$$

As an example, the first three u_k 's turn out to be

$$\begin{aligned} u_1 &= -j \int_0^z (|u_0|^2 u_0) \otimes h(z - \zeta, t) e^{-\alpha\zeta} d\zeta, \\ u_2 &= -j \int_0^z (2|u_0|^2 u_1 + u_0^2 u_1^*) \otimes h(z - \zeta, t) e^{-\alpha\zeta} d\zeta, \\ u_3 &= -j \int_0^z (2|u_0|^2 u_2 + u_0^2 u_2^* + 2|u_1|^2 u_0 + u_1^2 u_0^*) \otimes h(z - \zeta, t) e^{-\alpha\zeta} d\zeta. \end{aligned}$$

Turning again our attention to (9), we note that it suggests the following recurrence relation

$$\begin{aligned} v_0(z, t) &= u_0(z, t) \\ v_{n+1}(z, t) &= u_0(z, t) - j\gamma \int_0^z [|v_n(\zeta, t)|^2 v_n(\zeta, t)] \otimes h(z - \zeta, t) e^{-\alpha\zeta} d\zeta \end{aligned} \quad (13)$$

and it is easy to see that

$$\lim_{n \rightarrow \infty} v_n(z, t) = u(z, t) \quad (14)$$

as it can be shown that

$$\left. \frac{1}{k!} \frac{\partial^k v_n(z, t)}{\partial \gamma^k} \right|_{\gamma=0} = u_k(z, t), \quad 0 \leq k \leq n. \quad (15)$$

This means that the rate of convergence of (13) is not greater than that of (10) when using the same number of terms as the recurrence steps, i.e., it is poor [9]. We will now seek an improved recurrence relation with an accelerated rate of convergence to the solution of (2).

4. AN IMPROVED RECURRENCE RELATION CORRESPONDING TO A LOGARITHMIC PERTURBATION METHOD

As shown in [10], a faster convergence rate is obtained when expanding in power series in γ the log of $u(z, t)$ rather than $u(z, t)$ itself as done in (10). So, we try to recast (9) in terms of $\log u(z, t)$, and to this end rewrite it as

$$\frac{u(z, t) - u_0(z, t)}{u_0(z, t)} = -\frac{j\gamma}{u_0(z, t)} \int_0^z [|u(\zeta, t)|^2 u(\zeta, t)] \otimes h(z - \zeta, t) e^{-\alpha\zeta} d\zeta. \quad (16)$$

Using now the expansion

$$\log \frac{u}{u_0} = \frac{u - u_0}{u_0} - \frac{1}{2} \left(\frac{u - u_0}{u_0} \right)^2 + \frac{1}{3} \left(\frac{u - u_0}{u_0} \right)^3 - \dots \quad (17)$$

we replace the term $(u - u_0)/u_0$ in (16), obtaining

$$\log \frac{u}{u_0} = -\frac{j\gamma}{u_0} \int_0^z [|u|^2 u] \otimes h e^{-\alpha\zeta} d\zeta - \frac{1}{2} \left(\frac{u - u_0}{u_0} \right)^2 + \frac{1}{3} \left(\frac{u - u_0}{u_0} \right)^3 - \dots \quad (18)$$

where, for simplicity, we omitted all the function arguments. So, the sought improved recurrence relation suggested by (18) is

$$\begin{aligned} v_0 &= u_0 \\ v_{n+1} &= v_n \exp \left\{ -\frac{j\gamma}{v_0} \int_0^z [|v_n|^2 v_n] \otimes h(z - \zeta, t) e^{-\alpha\zeta} d\zeta - \frac{v_n - v_0}{v_0} \right\} \end{aligned} \quad (19)$$

where we used again (17) to obtain the right side of the second equation. Also in this case $\lim_{n \rightarrow \infty} v_n(z, t) = u(z, t)$, as it can be shown that the power series in γ of $\log v_n(z, t)$ coincides with that of $\log u(z, t)$ in the first n terms.

Notice that $v_1(z, t)$ evaluated from (19) coincides with the first-order multiplicative approximation in [10], there obtained with a different approach. The method in [10] is really a logarithmic perturbation (LP) method as the solution $u(z, t)$ is written as

$$u(z, t) = u_0(z, t)e^{-j\gamma\vartheta(z, t)}, \quad \vartheta = \vartheta_0 + \gamma\vartheta_1 + \gamma^2\vartheta_2 + \dots \quad (20)$$

and $\vartheta_0(z, t)$, $\vartheta_1(z, t)$ are evaluated by analytically approximating the SSFM solution. The calculation of $\vartheta_n(z, t)$ becomes progressively more involved for increasing values of n , but that method is useful because it can provide an analytical expression for the SSFM errors due to a finite step size [10].

We now follow another approach. Letting

$$\psi_n(z, t) \triangleq -j\vartheta_{n-1}(z, t), \quad (21)$$

such that

$$u(z, t) = u_0(z, t) \exp(\gamma\psi_1(z, t) + \gamma^2\psi_2(z, t) + \gamma^3\psi_3(z, t) + \dots), \quad (22)$$

for every n , $\psi_n(z, t)$ can be easily evaluated in the following manner. The power series expansion of $u(z, t)$ in (22) is

$$\begin{aligned} u_0 \exp\left(\sum_{k=1}^{\infty} \gamma^k \psi_k\right) &= u_0 \sum_{i=0}^{\infty} \frac{1}{i!} \left(\sum_{k=1}^{\infty} \gamma^k \psi_k\right)^i \\ &= u_0 \left[1 + \sum_{n=1}^{\infty} \left(\sum_{k=1}^n \frac{\varphi_{n,k}}{k!}\right) \gamma^n\right] \end{aligned} \quad (23)$$

where

$$\varphi_{n,k} = \begin{cases} 0 & \text{if } n \neq 0, k = 0 \\ 1 & \text{if } n = k = 0 \\ \sum_{m=k-1}^{n-1} \varphi_{m,k-1} \psi_{n-m} & \text{otherwise} \end{cases} \quad (24)$$

Equating (10) to (23), and taking into account that $\varphi_{n,1} = \psi_n$, we can recursively evaluate the ψ_n 's as

$$\psi_n = \frac{u_n}{u_0} - \sum_{k=2}^n \frac{\varphi_{n,k}}{k!}. \quad (25)$$

Thus, from the n -th order regular perturbation approximation we can construct the n -th order logarithmic perturbation approximation. As an example we have

$$\begin{aligned}\psi_1 &= \frac{u_1}{u_0}, \\ \psi_2 &= \frac{u_2}{u_0} - \frac{1}{2}\psi_1^2, \\ \psi_3 &= \frac{u_3}{u_0} - \psi_1\psi_2 - \frac{1}{6}\psi_1^3, \\ \psi_4 &= \frac{u_4}{u_0} - \psi_1\psi_3 - \frac{1}{2}\psi_2^2 - \frac{1}{2}\psi_1^2\psi_2 - \frac{1}{24}\psi_1^4.\end{aligned}$$

So, once evaluated the u_k 's from (12), we can evaluate the ψ_k 's from (25) and then $u(z, t)$ through (22), unless $u_0(z, t)$ is zero (or very small), in which case we simply use (10) as in this case $u(z, t)$ is also small and (10) is equally accurate.

5. COMPUTATIONAL ISSUES

The computational complexity of (12), (13) and (19) is the same, and at first glance it may seem that a n -th order integral must be computed for the n -th order approximation. However, it is not so and the complexity only increases linearly with n . Indeed, the terms depending on z can be taken out of the integration² and so all the integrals can be computed in parallel. However, only for $n \leq 2$ these methods turn out to be faster than the SSFM because of the possibility to exploit efficient quadrature rules for the outer integral, whereas the inner ones are to be evaluated through the trapezoidal rule as, to evaluate them in parallel, we are forced to use the nodes imposed by the outer quadrature rule.

Although (12), (13), (19), and (22) hold for a single fiber span, they can also be used in the case of many spans with given dispersion maps and per-span amplification. Indeed, one simply considers the output signal at the end of each span as the input signal to the next span [9, 10]. We would like to point out that even if the propagation in the compensating fiber is considered to be linear, (19) or (22) should still be used for the total span length L , by simply replacing z with the length of the transmission fiber L_F in the upper limit of integration and with L in all other places.

²This is apparent when performing the integrals in the frequency domain, but is also true in the time domain as $h(z - \zeta, t) = h(z, t) \otimes h(-\zeta, t)$ when $h(\ell, t)$ is the impulse response of a linear fiber of length ℓ ($h(-\zeta, t)$ simply corresponds to a fiber of length ζ and opposite sign of dispersion parameter).

6. SOME RESULTS

To illustrate the results obtainable by the RP and LP methods, we considered a $n \times 100$ km link, composed of n 100 km spans of transmission fiber followed by a compensating fiber and per span amplification recovering all the span loss. The transmission fiber is a standard single-mode fiber with $\alpha = 0.19$ dB/km, $D = 17$ ps/nm/km, $\gamma = 1.3$ W⁻¹km⁻¹, whereas the compensating fiber has $\alpha = 0.6$ dB/km, $D = -100$ ps/nm/km, $\gamma = 5.5$ W⁻¹km⁻¹, and a length such that the residual dispersion per span is zero.

In Table 1 we report the minimum order of the RP and LP methods necessary to have a normalized square deviation (NSD) less than 10^{-3} . The NSD is defined as

$$\text{NSD} = \frac{\int |u_{SSFM}(z, t) - u_P(z, t)|^2 dt}{\int |u_{SSFM}(z, t)|^2 dt} \quad (26)$$

where $u_{SSFM}(z, t)$ is the solution obtained by the SSFM with a step size of 100 m, $u_P(z, t)$ is either the RP or LP approximation, and the integrals extend to the whole transmission period, which in our case is that corresponding to a pseudorandom bit sequence of length 64 bits. The input signal format is NRZ at 10 Gb/s, filtered by a Gaussian filter with bandwidth equal to 20 GHz.

Table 1. Minimum order of the RP and LP methods necessary to achieve $\text{NSD} < 10^{-3}$ for a given input peak power and number of spans.

Spans	3 dBm		6 dBm		9 dBm		12 dBm	
	RP	LP	RP	LP	RP	LP	RP	LP
1	1	1	1	1	1	1	2	1
2	1	1	1	1	2	1	3	2
3	1	1	1	1	2	1	3	2
4	1	1	1	1	2	1	3	2
5	1	1	2	1	2	1	3	2
6	1	1	2	1	2	1	3	2
7	1	1	2	1	2	2	3	2
8	1	1	2	1	3	2	3	2
9	1	1	2	1	3	2	3	3
10	1	1	2	1	3	2	4	4

It can be seen that the LP method requires a lower order than the RP method to achieve the same accuracy when the input peak power P_{in} increases beyond 6 dBm and the number of spans exceeds 4. As an example, Fig. 1 shows the output intensity for an isolated “1” in the pseudorandom sequence when the input peak power is 12 dBm and the number of spans is 5, showing that, in this case, 3rd-order is required for the RP method, whereas only 2nd-order for the LP method. As a matter of fact, until 12 dBm and 8 spans, the 2nd-order LP method suffices for a $\text{NSD} < 10^{-3}$. However, for higher values of P_{in}

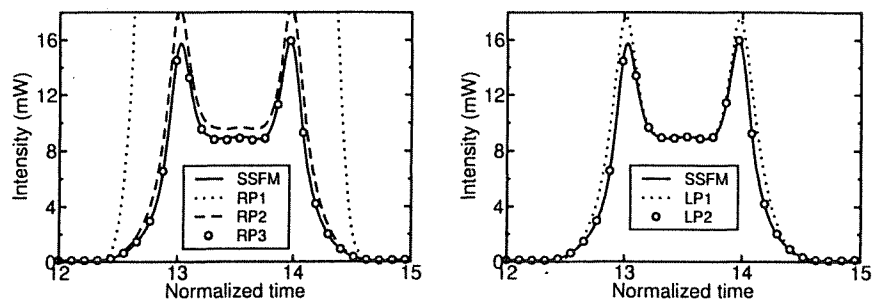


Figure 1. Output intensity for an isolated "1" with $P_{in} = 12$ dBm and 5 spans.

and number of spans, i.e., when moving from left to right along a diagonal in Table 1, the two methods tend to become equivalent, in the sense that they tend to require the same order to achieve a given accuracy.

This can be explained by making the analytical form (19) of the NLSE solution explicit. Indeed, doing so we can see that the nonlinear parameter γ appears at the exponent, and then at the exponent of the exponent, and then at the exponent of the exponent of the exponent, and so on. So, the LP approximation has an initial advantage over the RP one, but when orders higher than 3 or 4 are needed, this initial advantage is lost and the two approximations tend to coincide.

7. CONCLUSIONS

We presented two recurrence relations that asymptotically approach the solution of the NLSE. Although they represent an analytical expression of such solution, their computational complexity increases linearly with the recursion depth, making them not practical for a too high order of recursion. Nevertheless, for practical values of input power and number of spans, as those used in current dispersion managed systems, the second-order LP method can provide accurate results in a shorter time than the SSFM (we estimated an advantage of about 30% for approximately the same accuracy). Furthermore, we believe that these expressions can have a theoretical value, for example in explaining that the RP and LP methods are asymptotically equivalent, as we did.

REFERENCES

- [1] *Nonlinear fiber optics*. San Diego: Academic Press, 1989.
- [2] V. E. Zakharov and A. B. Shabat, "Exact theory for two-dimensional self-focusing and one-dimensional self-modulation of waves in nonlinear media," *Sov. Phys. JETP*, vol. 34, pp. 62–69, 1972.
- [3] N. N. Akhmediev, V. M. Elonskii, and N. E. Kulagin, "Generation of periodic trains of picosecond pulses in an optical fiber: exact solution," *Sov. Phys. JETP*, vol. 62, pp. 894–

- 899, 1985.
- [4] E. R. Tracy, H. H. Chen, and Y. C. Lee, "Study of quasiperiodic solutions of the nonlinear schrodinger equation and the nonlinear modulational instability," *Phys. Rev. Lett.*, vol. 53, pp. 218–221, 1984.
 - [5] M. Karlsson, "Modulational instability in lossy optical fibers," *J. Opt. Soc. Am. B*, vol. 12, pp. 2071–2077, Nov. 1995.
 - [6] A. Carena, V. Curri, R. Gaudino, P. Poggiolini, and S. Benedetto, "New analytical results on fiber parametric gain and its effects on ASE noise," *IEEE Photon. Technol. Lett.*, vol. 9, pp. 535–537, Apr. 1997.
 - [7] R. Hui, M. O'Sullivan, A. Robinson, and M. Taylor, "Modulation instability and its impact in multispans optical amplified imdd systems: theory and experiments," *J. Lightwave Technol.*, vol. 15, pp. 1071–1082, July 1997.
 - [8] C. Lorattanasane and K. Kikuchi, "Parametric instability of optical amplifier noise in long-distance optical transmission systems," *IEEE J. Quantum Electron.*, vol. 33, pp. 1058–1074, July 1997.
 - [9] A. Vannucci, P. Serena, and A. Bononi, "The RP method: a new tool for the iterative solution of the nonlinear Schrödinger equation," *J. Lightwave Technol.*, vol. 20, pp. 1102–1112, July 2002.
 - [10] E. Ciaramella and E. Forestieri, "Analytical approximation of nonlinear distortions," *IEEE Photon. Technol. Lett.*, 2004. To appear.
 - [11] A. V. T. Cartaxo, "Small-signal analysis for nonlinear and dispersive optical fibres, and its application to design of dispersion supported transmission systems with optical dispersion compensation," *IEE Proc.-Optoelectron.*, vol. 146, pp. 213–222, Oct. 1999.
 - [12] H. Hasegawa and Y. Kodama, *Solitons in Optical Communications*. New York: Oxford University Press, 1995.
 - [13] K. V. Peddanarappagari and M. Brandt-Pearce, "Volterra series transfer function of single-mode fibers," *IEEE J. Lightwave Technol.*, vol. 15, pp. 2232–2241, Dec. 1997.

MODULATION AND DETECTION TECHNIQUES FOR DWDM SYSTEMS*

Invited Paper

Joseph M. Kahn¹ and Keang-Po Ho²

¹Stanford University, Department of Electrical Engineering, Stanford, CA 94305 USA, e-mail: jmk@ee.stanford.edu; ²National Taiwan University, Institute of Communication Engineering and Department of Electrical Engineering, Taipei 106, Taiwan, e-mail: kpho@cc.ee.ntu.edu.tw

Abstract: Various binary and non-binary modulation techniques, in conjunction with appropriate detection techniques, are compared in terms of their spectral efficiencies and signal-to-noise ratio requirements, assuming amplified spontaneous emission is the dominant noise source. These include (a) pulse-amplitude modulation with direct detection, (b) differential phase-shift keying with interferometric detection, (c) phase-shift keying with coherent detection, and (d) quadrature-amplitude modulation with coherent detection.

Key words: optical fiber communication; optical modulation; optical signal detection; differential phase-shift keying; phase-shift keying; pulse amplitude modulation; heterodyning; homodyne detection.

1. INTRODUCTION

Currently deployed dense wavelength-division-multiplexed (DWDM) systems use binary on-off keying (OOK) with direct detection. In an effort to improve spectral efficiency and robustness against transmission impairments, researchers have investigated a variety of binary and non-binary modulation techniques, in conjunction with various detection techniques. In this paper, we compare the spectral efficiencies and signal-to-noise ratio (SNR) requirements of several modulation and detection techniques. We assume that amplified spontaneous emission (ASE) from optical amplifiers is the dominant noise

*This research was supported at Stanford University by National Science Foundation Grant ECS-0335013 and at National Taiwan University by National Science Council of R.O.C. Grant NSC-92-2218-E-002-034.

source. We do not explicitly consider the impact of other impairments, such as fiber nonlinearity (FNL), chromatic dispersion (CD), or polarization-mode dispersion (PMD).

The information bit rate per channel in one polarization is given by

$$R_b = R_s R_c \log_2 M, \quad (1)$$

where R_s is the symbol rate, $R_c \leq 1$ is the rate of an error-correction encoder used to improve SNR efficiency, and M is the number of transmitted signals that can be distinguished by the receiver. For an occupied bandwidth per channel B , avoidance of intersymbol interference requires $R_s \leq B$ [1]. If the channel spacing is Δf , the spectral efficiency per polarization is

$$S = \frac{R_b}{\Delta f} = \frac{R_s R_c \log_2 M}{\Delta f} \leq \frac{B R_c \log_2 M}{\Delta f} \quad (2)$$

Our figure of merit for spectral efficiency is $\log_2 M$, the number of coded bits per symbol, which determines spectral efficiency at fixed $R_s/\Delta f$ and fixed R_c . Binary modulation ($M = 2$) can achieve spectral efficiency up to 1 b/s/Hz, while non-binary modulation ($M > 2$) can achieve higher spectral efficiencies.

Non-binary modulation can improve tolerance to uncompensated CD and PMD, as compared to binary modulation, for two reasons [2, 3]. At a given bit rate R_b , non-binary modulation can employ lower symbol rate R_s , reducing signal bandwidth B , thus reducing pulse spreading caused by CD. Also, because non-binary modulation employs longer symbol interval $1/R_s$, it can often tolerate greater pulse spreading caused by CD and PMD.

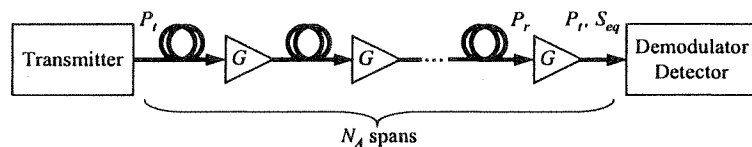


Figure 1. Equivalent block diagram of multi-span system.

In comparing SNR efficiencies, we consider the reference system shown in Fig. 1. The system comprises N_A fiber spans, each of gain $1/G$, and each followed by an amplifier of gain G . The average transmitted power per channel is P_t , while the average power at the input of each amplifier is $P_r = P_t/G$. We assume that for all detection schemes, ASE dominates over other noise sources, thereby maximizing the receiver signal-to-noise ratio (SNR) [4]. At the output of the final amplifier, the ASE in one polarization has a power spectral density

(PSD) given by

$$S_{eq} = N_A(G - 1)n_{sp}h\nu = (G - 1)n_{eq}h\nu, \quad (3)$$

where n_{sp} is the spontaneous emission noise factor of one amplifier, and we define the equivalent noise factor of the multi-span system by $n_{eq} = N_A n_{sp}$.

At the input of the final amplifier, the average energy per information bit is $E_b = P_r/R_b$. At the output of the final amplifier, the average energy per information bit is $GE_b = GP_r/R_b = P_t/R_b$, identical to the average transmitted energy per information bit. Our figure of merit for SNR efficiency is the value of the received SNR per information bit GE_b/S_{eq} required to achieve an information bit-error ratio (BER) $P_b = 10^{-9}$. This figure of merit indicates the average energy that must be transmitted per information bit for fixed ASE noise, making it appropriate for systems in which transmitted energy is constrained by FNL. Defining the average number of photons per information bit at the input of the final amplifier $n_b = E_b/h\nu$, and using (3), the figure of merit for SNR efficiency is

$$\frac{GE_b}{S_{eq}} = \left(\frac{G}{G - 1} \right) \frac{n_b}{n_{eq}} \approx \frac{n_b}{n_{eq}}, \quad (4)$$

which is equal to the receiver sensitivity at the final amplifier input divided by the equivalent noise factor of the multi-span system.

The modulation techniques described below can be employed with various elementary pulse shapes, including non-return-to-zero (NRZ) or return-to-zero (RZ), and with various line codes, such as duobinary or carrier-suppressed RZ. In the absence of fiber nonlinearity, with proper CD compensation and matched filtering, the elementary pulse shape and line code do not affect the spectral efficiency and SNR figures of merit considered here.

2. DIRECT DETECTION OF PAM

When used with direct detection, M -ary pulse-amplitude modulation (PAM) encodes a block of $\log_2 M$ bits by transmitting one of M intensity levels. Henry [5] and Humblet and Azizoglu [6] analyzed the performance of 2-PAM (OOK) with optical preamplification and direct detection. In order to achieve $P_b = 10^{-9}$, 2-PAM requires $n_b/n_{eq} = 38$ with single-polarization filtering and $n_b/n_{eq} = 41$ with polarization diversity.

We are not aware of an exact performance analysis of M -PAM for $M \geq 4$. Neglecting all noises except the dominant signal-spontaneous beat noise, at each intensity level, the photocurrent is Gaussian-distributed, with a variance

proportional to the intensity. Setting the $M - 1$ decision thresholds at the geometric means of pairs of adjacent levels approximately equalizes the downward and upward error probabilities at each threshold. In order to equalize the error probabilities at the $M - 1$ different thresholds, the M intensity levels should form a quadratic series [7]. Assuming Gray coding, the BER is given approximately by

$$\begin{aligned}
 P_b &\approx \frac{1}{\log_2 M} Q \left(\sqrt{\frac{3 \log_2 M}{(2M - 1)(M - 1)} \frac{GE_b}{S_{eq}}} \right) \\
 &= \frac{1}{\log_2 M} Q \left(\sqrt{\frac{3 \log_2 M}{(2M - 1)(M - 1)} \frac{n_b}{n_{eq}}} \right). \quad (5)
 \end{aligned}$$

For $M = 2$, (5) indicates that $n_b/n_{eq} = 36$ is required for $P_b = 10^{-9}$, which is lower by 0.2 dB than the exact requirement $n_b/n_{eq} = 38$. For $M \geq 4$, (5) indicates that the SNR requirement increases by a factor $(3 \log_2 M)/[(2M - 1)(M - 1)]$, corresponding to penalties of 5.5, 10.7 and 15.9 dB for $M = 4, 8, 16$, respectively. To estimate SNR requirements of M -PAM with single-polarization filtering, we assume the exact requirement $n_b/n_{eq} = 38$ for $M = 2$, and add the respective penalties for $M = 4, 8, 16$.

3. INTERFEROMETRIC DETECTION OF DPSK

Both M -ary phase-shift keying (PSK) and differential phase-shift keying (DPSK) use signal constellations consisting of M points equally spaced on a circle. While M -PSK encodes each block of $\log_2 M$ bits in the phase of the transmitted symbol, M -DPSK encodes each block of $\log_2 M$ bits in the phase change between successively transmitted symbols [1].

For interferometric detection of 2-DPSK, a Mach-Zehnder interferometer with a delay difference of one symbol compares the phases transmitted in successive symbols, yielding an intensity-modulated output that is detected by a balanced optical receiver. In the case of M -DPSK, $M \geq 4$, a pair of Mach-Zehnder interferometers (with excess phase shifts of 0 and $\pi/2$) and a pair of balanced receivers are used to determine the in-phase and quadrature components of the phase change between successive symbols.

Tonguz and Wagner [8] showed that the performance of DPSK with optical amplification and interferometric detection is equivalent to standard differentially coherent detection [1]. 2-DPSK requires $n_b/n_{eq} = 20$ with single-polarization filtering and $n_b/n_{eq} = 22$ with polarization diversity to achieve $P_b = 10^{-9}$ [8]. The performance of M -DPSK for $M \geq 4$ with single-polarization filtering is described by the analysis in [1].

4. COHERENT DETECTION OF PSK AND QAM

In optical communications, “coherent detection” has often been used to denote any detection process involving photoelectric mixing of a signal and a local oscillator [9]. Historically, the main advantages of coherent detection were considered to be high receiver sensitivity and the ability to perform channel demultiplexing and CD compensation in the electrical domain [9]. From a current perspective, the principal advantage of coherent detection is the ability to detect information encoded independently in both in-phase and quadrature field components, increasing spectral efficiency. This advantage can be achieved only by using synchronous detection, which requires an optical or electrical phase-locked loop (PLL), or some other carrier-recovery technique. Hence, we use the term “coherent detection” only to denote synchronous detection, which is consistent with its use in non-optical communications [1].¹

In ASE-limited systems, the sensitivity of a synchronous heterodyne receiver is equivalent to a synchronous homodyne receiver provided that the ASE is narrow-band-filtered or that image rejection is employed [10]. Most DWDM systems use demultiplexers that provide narrow-band filtering of the received signal and ASE, in which case, image rejection is not required for heterodyne to achieve the same performance as homodyne detection.

Both homodyne and heterodyne detection require polarization tracking or polarization diversity. Our analysis assumes tracking, as it requires fewer photodetectors. Coherent system performance is optimized by using high amplifier gain G and a strong local-oscillator laser, so that local-oscillator-ASE beat noise dominates over receiver thermal noise and other noise sources [4]. This corresponds to the standard case of additive white Gaussian noise [1].

M -ary PSK uses a constellation consisting of M points equally spaced on a circle. In the case of uncoded 2- or 4-PSK, the BER is given by [1]

$$P_b = Q\left(\sqrt{\frac{2GE_b}{S_{eq}}}\right) = Q\left(\sqrt{\frac{2n_b}{n_{eq}}}\right), \quad (6)$$

where the Q function is defined in [1]. Achieving a BER 10^{-9} requires $n_b/n_{eq} = 18$. The BER performance of M -PSK, $M > 4$ is computed in [1].

M -ary quadrature-amplitude modulation (QAM) uses a set of constellation points that are roughly uniformly distributed within a two-dimensional region. In the cases $M = 2^{2m}$ ($M = 4, 16, \dots$), the points are evenly arrayed in a

¹We do not consider heterodyne or phase-diversity homodyne detection with differentially coherent (delay) demodulation of DPSK, since the interferometric detection scheme described in Section 3 is mathematically equivalent [8] and is easier to implement. Likewise, we do not consider heterodyne or phase-diversity homodyne detection with noncoherent (envelope) demodulation of PAM, since the direct detection scheme described in Section 2 is mathematically equivalent [8] and is more easily implemented.

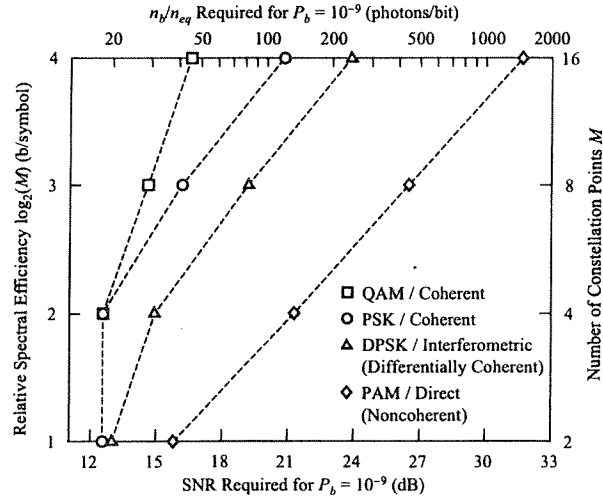


Figure 2. Spectral efficiency vs. SNR requirement for various techniques.

Table 1. Comparison of modulation and detection schemes. Numbers given represent the values of $GE_b/S_{eq} = n_b/n_{eq}$ (photons/bit) required for $P_b = 10^{-9}$. Numbers in parenthesis are the corresponding values of $10 \log_{10}(GE_b/S_{eq}) = 10 \log_{10}(n_b/n_{eq})$.

M	$\log_2 M$	PSK/Coherent One Pol.	QAM/Coherent One Pol.	DPSK/Interferometric		PAM/Direct	
				One Pol.	Two Pol.	One Pol.	Two Pol.
2	1	18 (12.6)	Not applicable	20 (13.0)	22 (13.4)	38 (15.8)	41 (16.1)
4	2	18 (12.6)	18 (12.6)	31 (14.9)	?	134 (21.3)	?
8	3	41 (16.2)	29 (14.6)	83 (19.2)	?	443 (26.5)	?
16	4	119 (20.8)	45 (16.6)	240 (23.8)	?	1472 (31.7)	?

$2^m \times 2^m$ square, while in the cases $M = 2^{2m+1}$ ($M = 8, 32, \dots$), the points are often arranged in a cross. The BER performance of M -QAM is computed in [1].

5. DISCUSSION

Fig. 2 and Table 1 compare the spectral efficiencies and SNR requirements of the various modulation and detection techniques described above. We observe that for $M > 2$, the SNR requirement for PAM increases very rapidly, while the SNR requirements of the other three techniques increase at a more moderate rate. Note that for large M , the SNR requirements increase with roughly equal slopes for PAM, DPSK and PSK, while QAM exhibits a distinctly slower increase of SNR requirement. This behavior can be traced to

Table 2. Comparison of detection techniques. Shading denotes an advantage.

Attribute	Direct	Interferometric	Coherent
Maximum degrees of freedom per polarization	1	1	2
Signal-to-noise requirement for binary modulation (relative to 2-PAM with direct detection)	0 dB (2-PAM)	-2.8 dB (2-DPSK)	-3.2 dB (2-PSK)
Signal-to-noise requirement for quaternary modulation (relative to 2-PAM with direct detection)	+5.5 dB (4-PAM)	-0.9 dB (4-DPSK)	-3.2 dB (4-PSK)
Electrical filtering can select WDM channel	No	No	Yes
Chromatic dispersion is linear distortion, making electrical compensation more effective	No	No	Yes
Local oscillator laser required at receiver	No	No	Yes
Polarization control or diversity required	No	No	Yes

the fact that PAM, DPSK and PSK offer one degree of freedom per polarization (either magnitude or phase), while QAM offers two degrees of freedom per polarization (both in-phase and quadrature field components). Based on Fig. 2, at spectral efficiencies below 1 b/s/Hz per polarization, 2-PAM (OOK) and 2-DPSK are attractive techniques. Between 1 and 2 b/s/Hz, 4-DPSK and 4-PSK are perhaps the most attractive techniques. At spectral efficiencies above 2 b/s/Hz, 8-PSK and 8- and 16-QAM become the most attractive techniques.

Table 2 compares key attributes of direct, interferometric and coherent detection. The key advantages of interferometric detection over direct detection lie in the superior SNR efficiency of 2- and 4-DPSK as compared to 2- and 4-PAM. Coherent detection is unique in offering two degrees of freedom per polarization, leading to outstanding SNR efficiency for 2- and 4-PSK, and still reasonable SNR efficiency for 8-PSK and for 8- and 16-QAM. Coherent detection also enables electrical channel demultiplexing and CD compensation. Coherent detection requires a local oscillator laser and polarization control, which are significant drawbacks.

Laser phase noise has traditionally been a concern for optical systems using DPSK, PSK or QAM. Interferometric detection of DPSK can be impaired by changes in laser phase between successive symbols. In coherent detection of PSK or QAM, a PLL (optical or electrical) attempts to track the laser phase noise, but the PLL operation is corrupted by ASE noise. Linewidth requirements for 2-DPSK, 2-PSK and 4-PSK are summarized in Table 3. At a bit rate $R_b = 10$ Gb/s, the linewidth requirements for 2-DPSK and 2-PSK can be accommodated by standard distributed-feedback lasers. 4-PSK requires a much narrower linewidth, which can be achieved by compact external cavity lasers [14].

Table 3. Laser linewidth requirements for various modulation and detection techniques, assuming a 0.5 dB penalty. For interferometric detection, transmitter has linewidth $\Delta\nu$, while for coherent detection, each of the transmitter and local oscillator has linewidth $\Delta\nu$.

Modulation	Detection	$\Delta\nu/R_b$	$\Delta\nu$ for $R_b = 10$ Gb/s	Reference
2-DPSK	Interferometric	3.0×10^{-3}	30 MHz	[11]
4-DPSK	Interferometric	?	?	
2-PSK	Coherent	8.0×10^{-4}	8 MHz	[12]
4-PSK	Coherent	2.5×10^{-5}	250 kHz	[13]

REFERENCES

- [1] J. G. Proakis, *Digital Communications, 4th Ed.*, McGraw-Hill, 2000.
- [2] S. Walklin and J. Conradi, "Multilevel signaling for increasing the reach of 10 Gb/s lightwave systems", *J. of Lightwave Technol.*, vol. 17, pp. 2235–2248, 1999.
- [3] J. Wang and J. M. Kahn, "Impact of chromatic and polarization-mode dispersions on DPSK systems using interferometric demodulation and direct detection", *J. Lightwave Technol.* vol. 22, no. 2, pp. 362–371, Feb. 2004.
- [4] E. Desurvire, *Erbium-Doped Fiber Amplifiers: Principles and Applications*, Wiley, 1994.
- [5] P. S. Henry, "Error-rate performance of optical amplifiers", *Proc. of Conf. on Optical Fiber Commun.*, Washington, DC, 1989, p. 170.
- [6] P. A. Humblet and M. Azizoglu, "On the bit error rate of lightwave systems with optical amplifiers", *J. Lightwave Technol.*, vol. 9, pp. 1576–1582, 1991.
- [7] J. Rebola and A. Cartaxo, "Optimization of level spacing in quaternary optical communication systems", *Proc. of SPIE*, vol. 4087, pp. 49–59, 2000.
- [8] O. K. Tonguz and R. E. Wagner, "Equivalence between preamplified direct detection and heterodyne receivers", *IEEE Photon. Technol. Lett.*, vol. 3, pp. 835–837, 1991.
- [9] G. P. Agrawal, *Fiber Optic Communication Systems, 3rd Ed.*, Wiley, 2002.
- [10] B. F. Jorgensen, B. Mikkelsen and C. J. Mahon, "Analysis of optical amplifier noise in coherent optical communication systems with optical image rejection receivers", *J. of Lightwave Technol.*, vol. 10, pp. 660–671, 1992.
- [11] C. P. Kaiser, P. J. Smith and M. Shafi, "An improved optical heterodyne DPSK receiver to combat laser phase noise", *J. Lightwave Technol.*, vol. 13, pp. 525–533, Mar. 1995.
- [12] S. Norimatsu and K. Iwashita, "Linewidth requirements for optical synchronous detection systems with nonnegligible loop delay time", *J. Lightwave Technol.*, vol. 10, pp. 341–349, Mar. 1992.
- [13] J. R. Barry and J. M. Kahn, "Carrier Synchronization for Homodyne and Heterodyne Detection of Optical Quadrature-Shift Keying", *J. Lightwave Technol.*, vol. 10, pp. 1939–1951, Dec. 1992.
- [14] J. D. Berger, Y. Zhang, J. D. Grade, H. Lee, S. Hrinya, H. Jerman, A. Fennema, A. Tselikov, and D. Anthon, "Widely tunable external cavity diode laser using a MEMS electrostatic rotary actuator", *Proc. of 27th Euro. Conf. on Optical Commun.* Amsterdam, Netherlands, Sept. 30-Oct. 4, 2001.

BEST OPTICAL FILTERING FOR DUOBINARY TRANSMISSION

Invited Paper

G. Bosco, A. Carena, V. Curri, and P. Poggiolini

Dipartimento di Elettronica, Politecnico di Torino, C.so Duca degli Abruzzi, 24 - 10129 Torino - Italy. E-mail:[lastname]@polito.it Tel. +39-011-5644036 Fax +39-011-5644099.

Abstract: We show that for optical transmission systems based on duobinary line-coding, in general the optimum receiver is not based on the optical filter matched to transmitted pulse-shape. In general, the receiver optical filter must be optimized for each transmitted pulse within the ISI conditions imposed by the duobinary line-coding. In order to achieve such a result, we have derived the expression of the parameter K to be maximized with the purpose to decide the optimal filter for each pulse-shape.

Key words: optical fiber communication; modulation formats; duobinary coding; quantum limit; optical filters.

1. INTRODUCTION

The duobinary format was first proposed in the 60's for radio communications [1]. Its high spectral efficiency was the aspect that made it attractive in that context. Later, duobinary was overcome by multilevel schemes that could reach an even higher bandwidth efficiency. Duobinary has recently re-emerged in the field of optical communications. Different implementations have been proposed, among which [2–5]. Comprehensive review papers on the advantages and disadvantages of the use of optical duobinary have been published, such as [6]. It has been pointed out that duobinary, besides a high bandwidth efficiency, also features a very high resilience to fiber chromatic dispersion.

Regarding the sensitivity performance of duobinary, diverging opinions exist. In [2] it was shown that a specific receiver performed in back-to-back equally well with either conventional IMDD or duobinary, suggesting a similar performance of the two formats. A more commonly acknowledged notion is

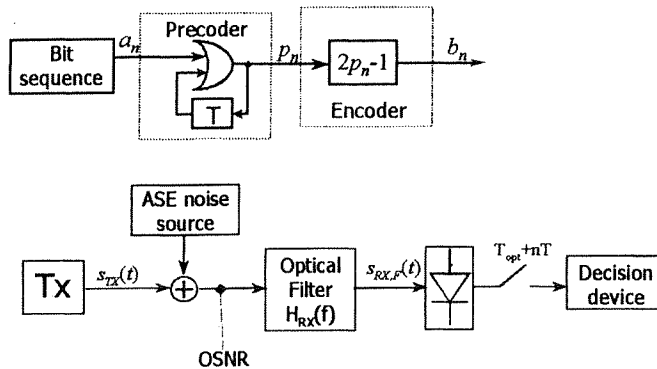


Figure 1. Duobinary transmitter architecture (top) and analyzed back-to-back system layout (bottom).

that duobinary may have a sensitivity penalty with respect to IMDD. In [7] we presented a rigorous analysis of the ASE-noise-limited, back-to-back sensitivity performance of duobinary, showing that the *quantum limit* [8] of duobinary is at least 0.91 dB *better* than that of IMDD.

After briefly recalling the derivation of such fundamental limit in Section 2, we focus on the pulse dependence of the bit-error rate which is a peculiar characteristic of duobinary transmission. In communication theory it has been shown that the optimum coherent receiver for intensity modulation systems is based on a filter matched to the transmitted pulse [9]. In general, this is valid also for optical systems based on intensity-modulation direct-detection (IMDD), even though a quadratic detector is used to perform optical-to-electrical conversion of the signal [10]. In this case the matched filter is the band-pass optical filter preceding the photodetector. In this work, we consider a simple use-case based on rectangular pulses and filter responses, and demonstrate that when choosing duobinary line-coding the matched-filter assumption is not valid in general. Moreover, we define the parameter K to be maximized in order to obtain the optimal receiver filter for a given pulse shape. For this parameter we report the analytical expression that can be used for any pulse-shape.

2. QUANTUM LIMIT FOR DUOBINARY

The duobinary TX structure (shown in Fig. 1) that can be found in early papers [11, 12] and in textbooks [9] is composed by a precoder, which transforms the information bit sequence a_n into a new bit sequence $p_n = a_n \oplus p_{n-1}$, where the symbol \oplus represents a logical *xor* operation, followed by the processing: $b_n = 2p_n - 1$. The bipolar sequence $b_n \in \{-1, 1\}$ is then used to create the

transmitted signal:

$$s_{TX}(t) = \sqrt{P_{S,av}} \sum_n b_n u(t - nT) e^{j2\pi f_o t} \hat{v}_p. \quad (1)$$

where $P_{S,av}$ is the average power of $s_{TX}(t)$. $u(t)$ is the normalized transmission pulse (with unitary power), T is the inverse of the bit-rate R_B and \hat{v}_p is the complex unit vector defining the polarization of the modulated signal. This signal can be either received using a coherent receiver or through direct-detection.

In optical communications, duobinary transmission is typically obtained taking advantage of the Mach-Zehnder modulator phase properties and of narrow electric filtering: it is called PSBT [4]. On the receiver side, a standard IMDD receiver is employed. We analyzed an optical duobinary system limited by ASE noise in back-to-back configuration as shown in Fig. 1. In [7], the duobinary application to optical communications has been analyzed showing that the received optical signal $s_{RX}(t)$ after the optical filter at the optimum sampling instant can be written as:

$$s_{RX}(t_{opt}) = \left\{ \sqrt{P_{S,av}} c_n x(0) + n_{pF}(t) \right\} \hat{v}_p + n_{oF}(t) \hat{v}_o. \quad (2)$$

where $c_n = 0$ if $b_n \neq b_{n-1}$ (i.e., $a_n = 0$) and $c_n = \pm 2$ if $b_n = b_{n-1}$ (i.e., $a_n = 1$). $n_{oF}(t) \hat{v}_o$ is the noise component on the polarization orthogonal to the modulated signal. Note that the received pulse $x(t)$ must comply with the duobinary ISI condition, i.e., $x(0) = x(T) \neq 0$ and $x(nT) = 0 \quad \forall n \neq 0, 1$.

The received optical signal is then converted to the decision electric signal by the photodetector. After photodetection, the noise component affecting the electrical signal at the optimum sampling instant can be modeled as a 4-degree of freedom Chi-square random process [7], with variance parameter:

$$\sigma^2 = \frac{N_0}{2} \int_{-\infty}^{+\infty} |H_{RX}(f)|^2 df \quad (3)$$

and non-centrality parameter $s^2 = 0$ if $b_n \neq b_{n-1}$ (i.e., $a_n = 0$) and $s^2 = 4P_{S,av}x^2(0)$ if $b_n = b_{n-1}$ (i.e., $a_n = 1$). $H_{RX}(f)$ is the frequency response of the receiver optical filter and N_0 is the one-side power spectral density of ASE noise before optical filtering, that in practical systems is set by the overall amount of noise introduced by the in-line optical amplifiers.

Accordingly to these characteristics of the decision signal and using the theory reported in [9], the expression for the Bit-Error-Rate (BER) for an optical duobinary system can be analytically written as:

$$\text{BER} = \frac{1}{2} \left\{ e^{-\phi} (1 + \phi) + 1 - Q_2 \left(\sqrt{\frac{4P_{S,av}x^2(0)}{\sigma^2}}, \sqrt{2\phi} \right) \right\}, \quad (4)$$

where Q_2 is the Marcum Q function of order 2 and ϕ is the decision threshold, that must be optimized for every value of the ratio $P_{S,av}x^2(0)/\sigma^2$. In any case, it can be shown that, independently of the value of ϕ , minimization of BER corresponds to maximization of the first argument of the Marcum Q_2 function. This argument is in fact strictly related to the optical signal-to-noise ratio (OSNR):

$$\frac{4P_{S,av}x^2(0)}{\sigma^2} = 16 \text{ OSNR} \frac{\frac{x^2(0)}{T}}{\int_{-\infty}^{+\infty} |H_{RX}(f)|^2 df} \quad (5)$$

where

$$\text{OSNR} = \frac{P_{S,av}}{2N_0R_B} \quad (6)$$

3. PULSE SHAPE DEPENDENCE OF BER

The analytical expression of the BER of optical duobinary is similar to that of IMDD [7], except now the first argument of the Q_2 depends on the pulse $x(t)$. This result means that, contrary to IMDD, for a given OSNR, different duobinary pulses may yield different BERs.

To appreciate this, we first assume the transmitted pulse $u(t)$ to be a rectangular pulse of duration T , i.e., the simplest and most typical NRZ pulse. $x(t)$ turns out to be a triangular pulse: $x(t) = 1 - |t/T - 1/2|$ for $t \in [-T/2, 3T/2]$ and $x(t) = 0$ for t outside $[-T/2, 3T/2]$. We get $x(0)/x(T/2) = 1/2$ which, by comparing it to the results presented in [7], shows that there is a penalty with respect to IMDD of exactly 3 dB.

We then select the duobinary pulse with the smallest possible bandwidth occupation [9, 11]:

$$x(t) = \frac{\cos\left(\pi\left[\frac{t}{T} - \frac{1}{2}\right]\right)}{\pi\frac{t}{T}\left(1 - \frac{t}{T}\right)} \quad (7)$$

Now we have $x(0)/x(T/2) = \pi/4$ and the resulting OSNR for $\text{BER} = 10^{-9}$ is 16.2, or 12.09 dB, with a *gain* with respect to IMDD of 0.91 dB. This result sets a new quantum limit of 32.4 photons per bit for a conventional optical direct-detection RX.

Between the two considered pulses there is a penalty of almost 4 dB, which shows that the choice of pulse shape is very critical for duobinary. At present, we have not been able to prove that the pulse yielding the lowest possible BER is (7), though we have not been able to find a better performing pulse either.

As a general consideration, we can say that, for any value of OSNR, the best pulse shape $u(t)$ and the best optical filter shape $H_{RX}(f)$ are a unique couple

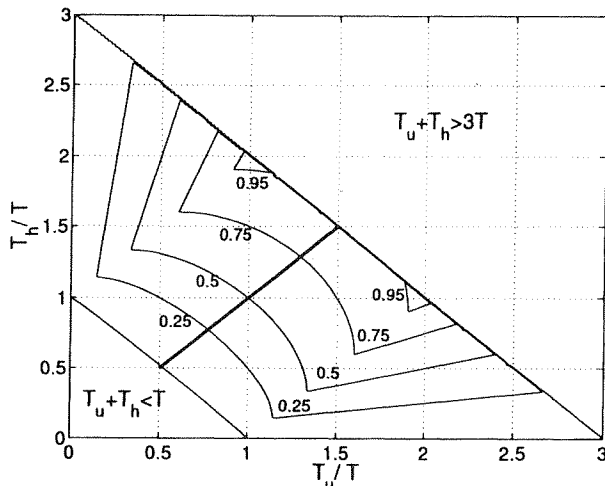


Figure 2. Contour plot of K as a function of both the normalized pulse duration of the transmitted pulse (T_u/T) and of the receiver optical filter impulse response (T_h/T)

and are the ones which maximize the ratio:

$$K = \frac{\frac{2x^2(0)}{T}}{\int_{-\infty}^{+\infty} |H_{RX}(f)|^2 df} = \frac{\frac{2}{T} \int_{-\infty}^{+\infty} u(t)h_{RX}(T/2 - t)dt}{\int_{-\infty}^{+\infty} |h_{RX}(t)|^2 dt} \quad (8)$$

It means that, unlike what happens in standard IMDD systems [10], the optimum receiver for duobinary is based on the pulse-filter pair that maximizes the parameter K .

In order to demonstrate that, in general, the optimum filter is not the one matched to the transmitted pulse shape, we have analyzed the behavior of the parameter K in a simple scenario for which analytical evaluations are straightforward. We assumed that both the transmitted pulse and the receiver optical filter impulse response have a rectangular shape with duration T_u and T_h , respectively. It is important to remark that, in order to comply with the duobinary ISI condition previously reported, T_u and T_h must satisfy the following two constraints [9]:

1. $T_u + T_h \leq 3T$ (otherwise $x(nT) \neq 0$ for some $n \neq 0, 1$);
2. $T_u + T_h > T$ (otherwise $x(0) = x(T) = 0$).

For each possible pair (T_u, T_h) , the value of K has been analytically evaluated for the considered scenario. Fig. 2 shows the contour plot of the parameter K as a function of the normalized duration of the transmitted pulse T_u/T and of the receiver optical filter impulse response T_h/T . Regions where $T_u + T_h < T$ and $T_u + T_h > 3T$ do not satisfy the duobinary ISI condition.

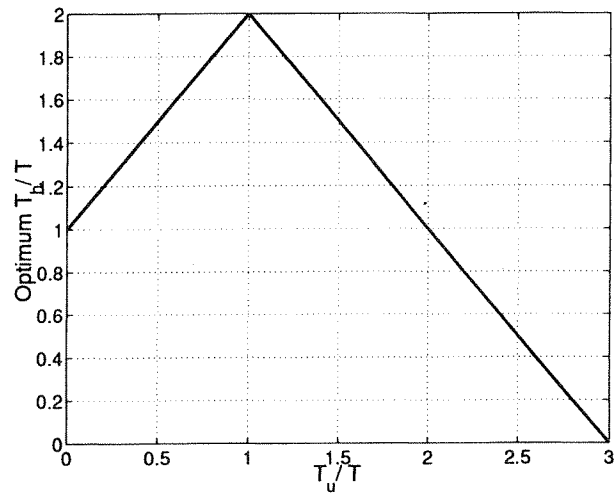


Figure 3. Plot of the optimum normalized impulse response duration (T_h/T) as a function of the normalized duration of the transmitted pulse (T_u/T).

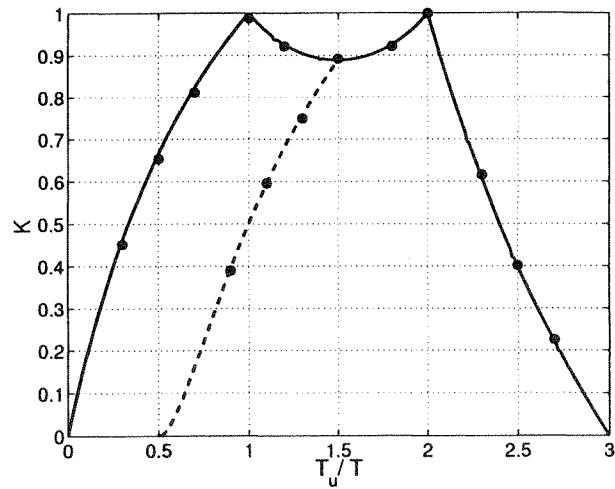


Figure 4. Plot of the optimum value of the parameter K as a function of T_u/T (solid line). Dotted line refers to the matched filter (sub-optimum) condition. Results reported as black dots are obtained through numerical simulation based on error counting.

The thick solid line corresponds to the case of optical filter matched to the transmitted pulse. Maximum values of K , i.e., optimal configurations, correspond to the two pairs ($T_u/T = 1, T_h/T = 2$) and ($T_u/T = 2, T_h/T = 1$), which do not belong to the matched filter category. It demonstrates that, in general, the optical matched filter is not the optimum for optical systems using duobinary line-coding. Similar counterexamples can be derived for other pulse and filter shapes.

Fig. 3 and Fig. 4 show as solid lines the optimum normalized filter duration T_h/T and the optimum value of K as a function of T_u/T , respectively. In Fig. 4, the dotted line refers to the matched filter condition: it can be noted that whenever a matched filter setup is a possible choice (i.e., in case $0.5 < T_u/T < 1.5$ so that the duobinary ISI condition is satisfied) there is always a better filtering option based on a narrower filter (longer impulse response duration).

As further verification, numerical simulations based on brute-force error-counting have been carried out: results are shown in Fig. 4 through black dots. A perfect agreement with the analytical results confirms the previous statements.

4. CONCLUSIONS

We have shown that for optical transmission systems based on duobinary line-coding, in general the optimum receiver is not based on the optical filter matched to transmitted pulse-shape. In general, the receiver optical filter must be optimized for each transmitted pulse within the ISI conditions imposed by the duobinary line-coding. In order to achieve such a result, we have derived the expression of the parameter K to be maximized with the purpose to decide the optimal filter for each pulse-shape.

REFERENCES

- [1] A. Lender, "The Duobinary technique for high-speed data transmission," *IEEE Trans. Commun. Technol.*, vol. 82, pp. 214–218, May 1963.
- [2] K. Yonenaga *et al.*, "Optical Duobinary transmission system with no receiver sensitivity degradation," *Electron. Lett.*, vol. 3, pp. 302–304, Feb. 1995.
- [3] X. Gu and L. C. Blank, "10 Gbit/s unrepeated optical transmission over 100 km of standard fibre," *Electron. Lett.*, vol. 29, pp. 2209–2211, 9 Dec. 1993.
- [4] D. Penninckx *et al.*, "The Phase-shaped Binary Transmission (PSBT): a new technique to transmit far beyond the chromatic dispersion limit," *Proc. ECOC '96*, Oslo, vol. 2, pp. 173–176.
- [5] H. Bissessur *et al.*, "3.2 Tb/s (80×40 Gb/s) C-band transmission over 3×100 km with 0.8 bit/s/Hz efficiency," in *Proc. ECOC'01*, Amsterdam, The Netherlands, 2001, Paper PD.M.1.11
- [6] T. Ono *et al.*, "Characteristics of optical Duobinary signals in terabit/s capacity, high-spectral efficiency WDM systems," *J. Lightwave Technol.*, vol. 16, pp. 788–797, May 1998.

- [7] G. Bosco, A. Carena, V. Curri, R. Gaudino, and P. Poggiolini, "Quantum limit of direct detection optically preamplified receivers using duobinary transmission", *IEEE Photon. Technol. Lett.*, vol. 15, no. 1, pp. 102–104, Jan. 2003.
- [8] P. J. Winzer, "Optically preamplified receiver with low quantum limit," *Electron. Lett.*, vol. 37, no. 9, p. 582, Apr. 2001.
- [9] J. G. Proakis, *Digital Communication*, New York: McGraw-Hill, 1989.
- [10] L. Kazovsky *et al.*, *Optical Fiber Communication Systems*, Artech House Inc., 1996.
- [11] E. R. Kretzmer, "Generalization of a technique for binary data communication," *IEEE Trans. Commun. Technol.*, vol. COM-14, pp. 67–68, Feb. 1966.
- [12] P. Kabal and S. Pasupathy, "Partial response signaling," *IEEE Trans. Commun.*, vol. COM-23, no. 9, pp. 921–934, Sep. 1975.

THEORETICAL LIMITS FOR THE DISPERSION LIMITED OPTICAL CHANNEL

Roberto Gaudino

Politecnico di Torino, Photonlab, Dipartimento di Elettronica, Corso Duca degli Abruzzi, 24, 10129 Torino, Italy

gaudino@polito.it

Abstract: In this paper, we study the theoretical limits of optical communication channels affected by chromatic dispersion. By using as a metric the energy transfer ratio, we find the optimal transmitted pulse shape that allows minimizing the impact of dispersion, together with an interesting definition of the dispersive channel equivalent bandwidth. This paper, though mainly theoretical, tries to approach using a rigorous formalism a problem that is currently receiving large interest, i.e., the optimization of the transmitter for a dispersion-limited optical system.

Key words: optical fiber communication; chromatic dispersion; intersymbol interference; energy transfer ratio.

1. INTRODUCTION

A large amount of theoretical and experimental work has recently focused on finding efficient modulation formats for the so-called “dispersion-limited” optical channel [1], i.e., for an optical link mainly limited by fiber chromatic dispersion. In this paper, we try to approach the problem using a rigorous theoretical formalism, by solving, under a suitable metric discussed below, the problem of the optimization of the transmitted input pulse which leads to the minimization of intersymbol interference (ISI) at the receiver. The paper is mainly theoretical, and allows to define an interesting equivalent bandwidth for the dispersion-limited channel. Anyway, it is also open to practical application, as mentioned in a previous paper [2].

2. MATHEMATICAL ASSESSMENT OF THE PROBLEM

Being interested in dispersion-limited systems, we focus on a fiber transmission model which includes first order chromatic dispersion only, neglecting all other transmission impairments. Thus, we consider the well-known chromatic dispersion transfer function [1]:

$$H_F(f) = e^{-j\frac{\beta_2}{2}L(2\pi f)^2} \quad (1)$$

where $\beta_2 = -\frac{\lambda_0 D}{2\pi f_0}$ is the *chromatic dispersion parameter*, being D the *fiber chromatic dispersion* (usually expressed in ps/nm/km), and λ_0 and f_0 the laser central wavelength and frequency, respectively, while L is the fiber length. As commonly accepted, we will indicate as *accumulated dispersion* the quantity $\beta_2 L$ in ps² or equivalently DL in ps/nm. We neglect higher order dispersion, such as β_3 .

In order to simplify the expressions, we introduce the *Normalized Dispersion Index* (NDI) γ ,¹ defined as:

$$\gamma = -2\beta_2 LR^2 \quad (2)$$

where $R = 1/T_B$ is the system bit rate (being T_B the bit duration). The γ parameter is quite useful in simplifying the equations, normalizing them to the system bit rate R or the bit duration T_B . In fact, using this notation, the transfer function and impulse response become [1]:

$$H_F(f) = e^{j\gamma\left(\frac{\pi f}{R}\right)^2} \rightarrow h_F(t) = \frac{e^{j\pi/4} \text{sign}(\gamma)}{T_B \sqrt{\pi|\gamma|}} e^{-j\frac{\gamma}{\pi}\left(\frac{t}{T_B}\right)^2}. \quad (3)$$

so that both time and frequency can be normalized to the bit rate R and bit duration T_B . We assume that the transmitted binary digital signal (complex envelope optical field) is in the form: $x(t) = \sum_{k=-\infty}^{+\infty} \alpha_k \cdot s_{in}(t - kT_B)$ where $s_{in}(t)$ is the complex envelope of the transmitted pulse for a single bit, and α_k assumes the values 0 and 1 for a standard OOK modulation. Since the channel is linear and time invariant (LTI), the resulting pulse at the fiber output is $s_{out}(t) = s_{in}(t) * h_F(t)$. The goal of our paper is the optimization of the input pulse $s_{in}(t)$ under the following assumptions:

- The input pulse $s_{in}(t)$ is strictly time-limited to the interval:

$$I = [-T_{in}/2, +T_{in}/2] \quad (4)$$

¹The γ parameter has already been used by other authors, such as [1], this γ should not be confused with the optical fiber nonlinear Kerr coefficient.

As a particular case, we have $T_{in} = T_B$ for a standard memoryless transmitter, but we will show that the case $T_{in} > T_B$, corresponding to a transmitter with memory, is extremely interesting in extending the dispersion limit. In particular, we will assume $T_{in} = n_{mem} \cdot T_B$, where the (integer) parameter n_{mem} is the transmitter memory. The extension of our results to a modulation with memory is the main new result of this paper with respect to our previous paper on the same topic [2]. Using modulation with memory, the pulse transmitted for each individual bit has a duration that extends beyond the one bit window, an approach that is typical in line coding, such as duobinary [1]. As a practical example, a system working at 10 Gbit/s ($T_B = 100$ ps) with $n_{mem} = 4$ will use pulses at the transmitter side with a duration $T_{in} = 400$ ps. The particular case $n_{mem} = 1$ corresponds to a standard, memoryless modulation. For $n_{mem} > 1$, it should be noted that the signal coming out of the transmitter is affected by ISI. Anyway, line coding is usually associated with a propagation channel that, under suitable conditions, reduces or cancels the amount of ISI present at the transmitter. For instance, optical duobinary can be interpreted as line coding with $n_{mem} = 2$. In fact, the resulting duobinary signal at the transmitter output is strongly affected by ISI, giving rise to a 3-level eye diagram. In the duobinary case, the ISI at the transmitter is anyway cancelled by the direct-detection receiver, which converts the 3-level ISI-affected signal into a standard 2-level signal without ISI. In general, in line coding or modulation with memory, a controlled amount of ISI is created at the transmitter in order to have some kind of advantage at the receiver.

- We chose as optimization criterion the maximization of the energy transfer from the input time window I to an output time window:

$$J = [-T_{out}/2, +T_{out}/2] \quad (5)$$

More specifically, we introduce the input and output energies:

$$\mathcal{E}_{in} = \int_I |s_{in}(t)|^2 dt \quad \text{and} \quad \mathcal{E}_{out} = \int_J |s_{out}(t)|^2 dt \quad (6)$$

and we maximize over $s_{in}(t)$ the *Energy Transfer Ratio* (ETR), defined as:

$$\text{ETR} = \frac{\mathcal{E}_{out}}{\mathcal{E}_{in}}. \quad (7)$$

The pulses $s_{in}(t)$ resulting from the optimization process proposed here will be indicated as “optimal pulses” in the rest of the paper.

- The criterion we have chosen is particularly relevant for the case $T_{out} = T_B$, if we assume symbol-by-symbol detection for a binary memoryless

receiver (i.e., a receiver taking decision on single received bits). The concentration of the output pulse energy over a T_B time window is effective in both minimizing ISI (which is the goal of our paper) and in increasing the signal to noise ratio at the decision instant for any “reasonable” digital receiver. In fact, the criterion is “exact” for an ideal optical integrate&dump receiver, since in this case the decision sample is directly proportional to the signal energy over a T_B time window. Anyway, as we we have shown in [2], it proves a extremely good criterion for realistic optical receiver structures. We notice that, for $n_{mem} > 1$, we are considering a somehow non-intuitive system where ISI is strongly present at the transmitter side, but then ISI is reduced, or even cancelled at the receiver side by the propagation over the dispersive channel.

- We will showed in [2] that the ETR (for $T_{out} = T_B$) for realistic optical receivers should typically be above 90% to give a penalty due to ISI in the 1-2 dB range. As a consequence, we will conventionally define in the rest of the paper the “dispersion limit” as the amount of accumulated dispersion for a given bit rate that results in an ETR = 90%.

2.1 The fundamental parameters and equations

The ETR optimization problem over a generic LTI system is a canonical problem that was studied in the past [3, 4] and can be reduced to the optimization of a quadratic functional in $s_{in}(t)$, with a quadratic constraint. For a generic filter impulse response, it leads to the following Fredholm integral equation of the second kind:

$$\int_I \mathcal{K}(u, v) s_{in}(u) du = \lambda s_{in}(v) \quad (8)$$

where the kernel of the integral equation is:

$$\mathcal{K}(u, v) = \int_J h_F(z - u) h_F^*(z - v) dz \quad (9)$$

and where the optimal solution is given by the eigenfunction corresponding to the *maximum eigenvalue* λ , which is equal to the ETR (7) [3].

This problem has been solved in the literature for several types of band-limited and standard low-pass filters [3–5]. In this paper, we solve it (for the first time to our knowledge) considering the fiber dispersive transfer function (1) as the band-limiting filter. In this case, replacing (3) in (9), by straightforward calculations, the kernel can be expressed as:

$$\mathcal{K}(u, v) = \frac{e^{-j\left(\frac{u^2 - v^2}{\gamma T_B^2}\right)}}{\pi(u - v)} \cdot \sin \left[\frac{T_{out}(u - v)}{|\gamma| T_B^2} \right]. \quad (10)$$

2.2 The closed form solution

The integral equation (8), with the kernel (10), can be solved by looking for a solution in the form $s_{in}(t) = a(t) \cdot e^{j\phi(t)}$, where $a(t)$ and $\phi(t)$ are real functions of time. This separates the two input pulse contributions that are usually called amplitude modulation and phase modulation (or chirp). In particular, we look for a solution of the form:

$$s_{in}(t) = a(t) \cdot e^{j\left(\frac{t}{T_B}\right)^2}. \quad (11)$$

This “guess” was originally driven by the observation of the numerical results obtained in [2], and proved to be exact, as shown in the following. By writing the kernel as $\mathcal{K}(u, v) = \mathcal{K}_{\mathcal{R}}(u, v) \cdot \exp\left[-j\left(\frac{u^2 - v^2}{\gamma T_B^2}\right)\right]$, where:

$$\mathcal{K}_{\mathcal{R}}(u, v) = \frac{1}{\pi(u - v)} \cdot \sin\left[\frac{T_{out}(u - v)}{|\gamma| T_B^2}\right] \quad (12)$$

and by substituting (11) into (8), the phase terms vanish and the resulting integral equation simplifies to:

$$\int_I \mathcal{K}_{\mathcal{R}}(u, v) a(u) du = \lambda a(v) \quad (13)$$

This is thus the fundamental integral equation that allows solving our optimization problem. It turns out that exactly the same integral equation results from the ETR pulse optimization over an ideal low-pass filter with bandwidth W and $J = [-\infty, +\infty]$. This is a very fortunate case, since the ideal low-pass filter problem received a lot of attention in the past, in the framework of fundamental works on communications theory, and it was fully analyzed and analytically solved in [5]. It leads to an integral equation with kernel:

$$\mathcal{K}_{LP}(u, v) = \frac{\sin[2\pi W(u - v)]}{\pi(u - v)}. \quad (14)$$

Thus, the integral equation (13) is mathematically equivalent to the ideal low-pass case. A full treatment of these results can be found in [6], [7], or in [8], where the expression of the result in terms of Prolate Spheroidal functions is given. In particular, it turns out that the solution corresponding to the the maximum eigenvalue of (13) corresponds to the one maximizing the ETR. By direct comparison between the kernels (12) and (14), we observe that we have the following equivalence among parameters:

$$2\pi W = \frac{T_{out}}{|\gamma| T_B^2} \Rightarrow W = \frac{T_{out}}{2\pi |\gamma| T_B^2}. \quad (15)$$

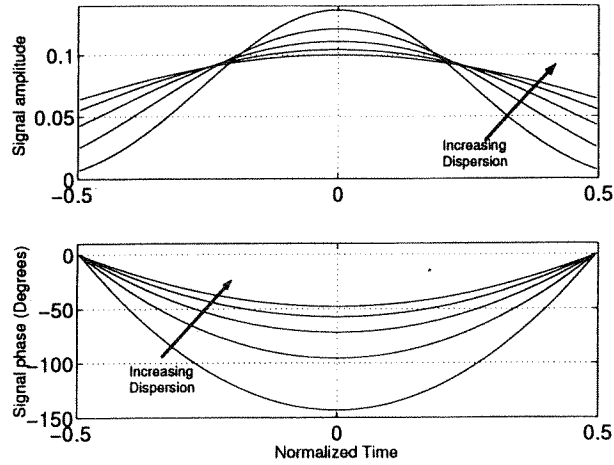


Figure 1. Optimal pulses for $n_{mem} = 1$ and γ values ranging from 0.1 to 0.3 in 0.05 steps. Time is normalized to T_B .

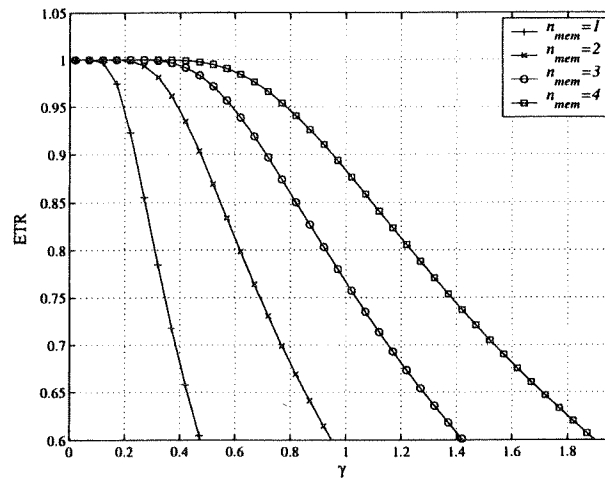


Figure 2. ETR vs. γ for $n_{mem} = 1, 2, 3, 4$.

The availability of a closed form solution is, in our opinion, the most important result of this paper, not only because it gives the optimal pulse expressed through prolate spheroidal functions [5], but even more because it leads to the interesting results we illustrate in the following Section. We show in Fig. 1 the resulting optimal pulses for $n_{mem} = 1$ and γ values ranging from 0.1 to 0.3 in 0.05 steps, while we show in Fig. 2 the ETR vs. γ for different n_{mem} values.

3. OPTIMAL CHIRP AND CHANNEL EQUIVALENT BANDWIDTH

The previous results lead to the following important considerations:

1. The optimal pulses have a phase modulation given by $\phi(t) = \frac{t^2}{\gamma T_B^2}$, or equivalently, $\phi(t) = -\frac{t^2}{2\beta_2 L}$. This expression gives the optimal chirp for pulses launched over a dispersive channel. Interestingly, this result was already found in [1] using a totally different approach for which anyway optimality was not proven.
2. Provided that the pulse chirp is chosen to be optimal, the dispersive channel is totally equivalent, at least in the ETR sense, to an ideal low-pass filter with bandwidth:

$$W = \frac{T_{out}}{2\pi|\gamma| T_B^2} \quad \text{or equivalently} \quad W = \frac{1}{4\pi|\beta_2|L} T_{out}. \quad (16)$$

This result can be usefully interpreted as a definition of the *equivalent bandwidth* of the dispersive channel which, to our knowledge, was never given before in a rigorous form. We note here that dispersive channel transfer function (1) has a peculiar expression that render most of the common bandwidth definitions totally useless, since $|H_F(f)|^2 = 1, \forall f$. For instance, the commonly used noise equivalent bandwidth is infinite, and the 3-dB bandwidth is meaningless.

3. In the ideal low-pass problem with kernel (14), it can be shown that the ETR depends *only* on WT_{in} , and the function $ETR = f(WT_{in})$ is monotonically increasing, asymptotically reaching $ETR = 1$ for $WT_{in} \rightarrow +\infty$ [5]. If we fix to the limiting value $ETR = 0.9$ (a 90% energy transfer), the condition $WT_{in} \geq 0.675$ must be satisfied [5]. In our case, using (16), the ETR is a function of $\frac{T_{out}T_{in}}{2\pi|\gamma| T_B^2}$ only. If we fix $T_{out} = T_B$ and $T_{in} = n_{mem} \cdot T_B$, we have that the ETR is only a function of $n_{mem}/|\gamma|$.
4. In order to have $ETR = 0.9$, for $n_{mem} = 1$, we have the condition $|\gamma| \leq 0.236$, or equivalently, introducing (2),

$$R^2 \leq \frac{0.1179}{|\beta_2 L|}. \quad (17)$$

This last equation can be interpreted as the theoretical upper bound to the maximum bit rate that can be achieved over the dispersive optical channel with limited ISI (i.e. $ETR = 0.9$) and for the memoryless modulator ($n_{mem} = 1$).

5. From another point of view, if we need to transmit over a fiber with arbitrary bit rate and dispersion, we can *always* obtain a limited ISI condition (e.g., $ETR \geq 0.9$) provided that we accept a memory n_{mem} at the transmitter given by:

$$n_{mem} \geq 4.241 |\gamma| \Rightarrow n_{mem} \geq 8.482 |\beta_2 L| R^2. \quad (18)$$

Table 1. Maximum acceptable accumulated dispersion values (in terms of DL in ps/nm) for 10 and 40 Gbit/s system for a given memory n_{mem} .

n_{mem}	10 Gbit/s	40 Gbit/s
1	928 ps/nm	58 ps/nm
2	1856 ps/nm	116 ps/nm
3	2785 ps/nm	174 ps/nm
4	3713 ps/nm	232 ps/nm

This is a novel and important result, stating that, we can limit ISI provided that the modulator memory n_{mem} is sufficiently large, and optimal pulses are used. Table 1 reports the amount of accumulated dispersion that, according to (18), can be tolerated for a 10 and 40 Gbit/s system for different n_{mem} .

The result expressed in (18) also states that the dispersive channel, for arbitrary values of dispersion, allows an arbitrarily high bit-rate, provided that n_{mem} is sufficiently large and, obviously, that optimal pulses are used. Practically, this means that for high dispersion, the optimal pulses are compressed by the channel from an input duration $n_{mem} \cdot T_B$ to an output duration close to $T_{out} = T_B$.

4. CONCLUSION

We have approached the problem of the optimization of the transmitted pulse in a dispersion-limited optical channel using a rigorous approach. We believe that our work, though mainly theoretical, can give a useful insight on the problem on optical line coding, and be a good complement of the approach followed in papers such as [1].

REFERENCES

- [1] E. Forestieri and G. Prati, "Novel optical line codes tolerant to fiber chromatic dispersion," *J. Lightwave Technol.*, vol. 19, no. 11, pp. 1675–1684, Nov. 2001.
- [2] R. Gaudino and E. Viterbo, "Pulse shape optimization in dispersion-limited direct detection optical fiber links," to appear on *IEEE Comm. Lett.*
- [3] M. Elia, G. Taricco, and E. Viterbo, "Optimal energy transfer in band-limited communication channels," *IEEE Trans. Inform. Theory*, vol. 45, no. 6, pp. 2020–2029, Sept. 1999.
- [4] L. E. Franks, *Signal Theory*, Prentice-Hall, 1969.
- [5] D. Slepian, "Some comments on Fourier analysis, uncertainty and modeling," *SIAM Rev.*, vol. 25, no. 3, pp. 379–393, July 1982.
- [6] D. Slepian and H. Pollak, "Prolate spheroidal wave functions, Fourier analysis and uncertainty - I", *Bell System Tech. J.*, vol. 40, pp. 43–63, Jan. 1961.
- [7] D. Slepian and H. Pollak, "Prolate spheroidal wave functions, Fourier analysis and uncertainty - II", *Bell System Tech. J.*, vol. 40, pp. 65–84, Jan. 1961.
- [8] *Data communication: fundamentals of baseband transmission*, Benchmark papers in Electrical Engineering and computer science, vol. 9, Halsted Press, 1974.

CAPACITY BOUNDS FOR MIMO POISSON CHANNELS WITH INTER-SYMBOL INTERFERENCE

Alfonso Martinez

Technische Universiteit Eindhoven; Electrical Eng. Dept., Signal Processing Group (SPS); Den Dolech 2, P. O. Box 513, 5600 MB Eindhoven, The Netherlands

alfonso.martinez@ieee.org

Abstract: We study multiple-access Poisson channels with multiple receivers. Each transmitter sends a sequence of modulated symbols, which may also be affected by inter-symbol interference. We derive some new formulas for the channel capacity, for the cases of both independent and coordinated transmission. We also provide some numerical results on the additional power required for efficient transmission due to the various sources of interference.

Key words: channel capacity; MIMO systems; intersymbol interference.

1. INTRODUCTION

A Poisson channel models an optical communication channel in which the fundamental impairment is shot noise. A signal is observed through a sequence of arrivals in a detector, and the arrivals follow a (random) Poisson process. Their position, which we also call arrival instants, counts, or time stamps, are known with arbitrarily good precision.

We shall study multiple-input multiple-output (MIMO) Poisson channels. A total of L signals are transmitted, denoted by $\lambda_l^T(t)$, with $1 \leq l \leq L$. These signals experience static mixing with coefficients by $H_{l,r}$, $1 \leq l \leq L$, $1 \leq r \leq R$; the mixing coefficients are real positive numbers, $H_{l,r} \geq 0$. The signals are detected by an array of R elements, each of them detecting a signal $\lambda_r(t) = \sum_{l=1}^L H_{l,r} \lambda_l^T(t)$. The arrival times at receiver r are denoted by τ_r .

Sect. 2 presents the capacity of an unconstrained MIMO channel, which corresponds to an ideal, non-dispersive, infinite-bandwidth system.

Some constraints typical of a practical optical channel are imposed in Section 3, where closed-form bounds to the capacity are presented and computed. Following standard practice, the signals are modulated with On-Off Keying (OOK), and are given by:

$$\lambda_i^T(t) = \sum_{n=0}^{N-1} A_i w_i(n) h(t - nT - \Delta_i). \quad (1)$$

With no loss of generality, we assume the following: A_i is the energy for the “on” symbol; $w_i(n) \in \{0, 1\}$ are the modulation symbols; $h(t)$ in the modulation pulse, real-valued, positive and of area 1; Δ_i is the relative delay of channel i ; a total of N symbols are transmitted. Note that dispersion is modelled as inter-symbol interference. Fig. 1 depicts the sequences transmitted in a system with two input channels.

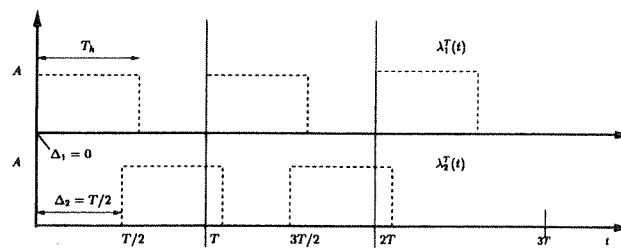


Figure 1. Transmitted signals: 2 OOK parallel channels.

2. UNCONSTRAINED MIMO POISSON CHANNEL

We extend the formula for single-input single-output (SISO) Poisson channel [1] with the following:

THEOREM 1: *For a Poisson channel with R receiver lines, the mutual information between the input intensity $\lambda(t) = ((\lambda_1(t), \dots, \lambda_R(t)))$, and the output $\underline{\tau} = (\underline{\tau}_1, \dots, \underline{\tau}_R)$ is given by:*

$$I(\lambda(t); \underline{\tau}) = \sum_{r=1}^R \int E_{\lambda_r(t)} \left\{ \psi(\lambda_r(t)) \right\} - E_{I_{\alpha}(t,r)} \left\{ \psi(\hat{\lambda}_r(t)) \right\} dt, \quad (2)$$

where $\psi(x) \triangleq x \log(x)$, $E_{I_{\alpha}(t,r)} \{ \cdot \}$ is the expectation over a past $I_{\alpha}(t, r)$ from instant t seen at receiver r , and $\hat{\lambda}_r(t)$ is defined as the expected value of the projection from the past $I_{\alpha}(t, r)$.

Note that the past $I_{\alpha}(t, r)$ is arbitrary, and need not be the causal ordering of time. The proof can be found in Appendix 2. The proof is constructive, and also provides a capacity-achieving input distribution. Similar to the SISO

channel (see Kabanov [1], Davis [2] and Wyner [3, 4]), a simple two-valued signal, such that all L signals are simultaneously active or inactive, is enough to achieve capacity. The distribution of the on and off states can be found in [3, 4]. If the signal duration is made ever smaller, all available degrees of freedom are used.

3. CONSTRAINED MIMO POISSON CHANNELS

In presence of modulation, we calculate the capacity per channel use, having defined a channel use as a symbol interval of duration T :

$$C = \sup_{\lambda(t)} \lim_{N \rightarrow +\infty} \frac{1}{N} I(\lambda(t); \underline{\tau}). \quad (3)$$

In practice, the limit will be truncated to a small value of N , and we shall assume that convergence in N has been achieved.

Even though (2) is a closed formula, it is not easily applicable to situations with bandwidth limitations, inter-symbol interference, and dispersion. The expectation operator $E_{I_{\alpha}(t,r)}\{\cdot\}$ is not easily tractable. Lapidoth and Moser [5] have recently calculated upper and lower bounds for the SISO discrete-time Poisson channel. They approximate the differential entropies in Eq. (4) by using some properties of Poisson rv. We are, however, interested in the continuous-time channel, for which their approximations fail.

An alternative route starts at the expression with the differential entropies (for a proof, see Appendix 2):

$$\begin{aligned} I(\lambda(t); \underline{\tau}) &= h(\underline{\tau}) - h(\underline{\tau}|\lambda(t)), \\ &= h(\underline{\tau}) + \sum_{r=1}^R \int E_{\lambda_r(t)} \{ \psi(\lambda_r(t)) \} dt - \sum_{r=1}^R \int E_{\lambda_r(t)} \{ \lambda_r(t) \} dt. \end{aligned} \quad (4)$$

Our calculations of the channel capacity will nevertheless involve several approximations:

- All symbols $w_i(n)$ are iid (no space-time coding). This is equivalent to having equiprobable signals $\lambda(t)$.
- Instead of the exact arrival times $\underline{\tau}$, we use the number of arrivals. We partition the time axis in disjoint intervals, and count the number of arrivals in each, which we denote by k_i , and \underline{k} for the whole partition. Due to the data processing inequality this may in general decrease the mutual information, as there may be information in the arrival instants. Appendix 2 elaborates on the relationship between the differential entropy $h(\underline{\tau})$ and the entropy $H(\underline{k})$, and the conditions under which they are equivalent.

Taken together, we obtain a lower bound to the channel capacity. Furthermore, as we are interested in symmetric situations, all users are assumed identical;

this implies in particular that there information rates and energies are identical. A simple upper bound is then obtained by considering the single-user capacity: the presence of other users cannot increase the average amount of information that can be transmitted.

Fig. 2 shows the capacity, measured in bits per symbol period (T), for an OOK scheme, and estimated with the equations presented above. The pulses have a length equal to T_h , as indicated in the plot, so that they may overlap with each other, a model for dispersion. The capacity is estimated in bits per symbol period, so that the maximum is 2, as there are two input channels. The channel matrix has a flat spatial response, $H_{l,r} = 0.5, l, r = 1, 2$. The second user has a delay $\Delta_2 = T/2$. Note that the model also corresponds to a situation with a single user corrupted by ISI. For comparison purposes, we also report the unconstrained capacity, and show the losses incurred by binary modulation, and then by multiple-access effects.

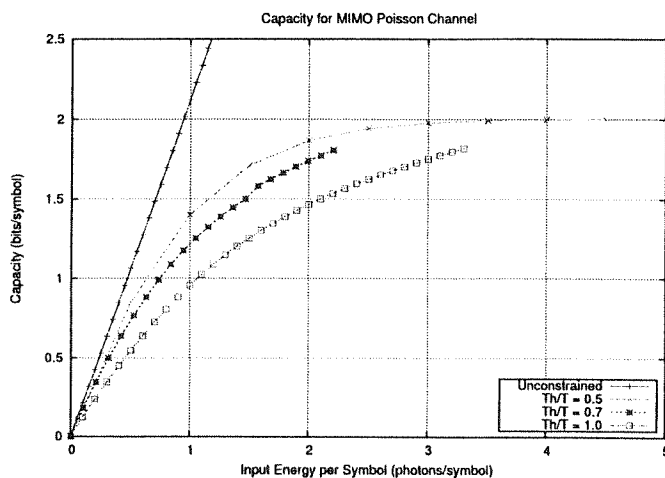


Figure 2. Capacity with OOK, from exact calculations and from simulations.

APPENDIX

The proof presented here is based on simple information-theoretic arguments, and as such differs from previous ones [1], which made use of martingales.

We start by stating two lemmas that will be used later. The proofs are sketchy, thanks to their simplicity.

LEMMA 2: *Let n be a Poisson random variable with parameter λ , where λ is itself randomly distributed in an interval $[0, A]$, $A \rightarrow 0$, with a density $p(\lambda)$. The conditional entropy $H(n|\lambda)$ is given by:*

$$H(n|\lambda) = \int_{\lambda} p(\lambda)(\lambda - \lambda \log \lambda) d\lambda = E\lambda - E\psi(\lambda) \quad (\text{A.1})$$

with $E\lambda = \int_0^A \lambda p(\lambda) d\lambda$, and $\psi(x) = x \log x$.

PROOF: As $A \rightarrow 0$, we can safely disregard second-order terms in A . The Poisson distribution tends to a Bernoulli variable, with only two possible values, 0 and 1. From the definition of entropy, in the limit $A \rightarrow 0$, and disregarding second order terms we obtain the desired expression. ■

LEMMA 3: Let n be a Poisson random variable with parameter λ , where λ is itself randomly distributed in an interval $[0, A]$, $A \rightarrow 0$, with a density $p(\lambda)$. The entropy $H(n)$ is given by:

$$H(n) = E\lambda - E\lambda \log E\lambda = E\lambda - \psi(E\lambda) \quad (\text{A.2})$$

with $E\lambda = \int_0^A \lambda p(\lambda) d\lambda$, and $\psi(x) = x \log x$.

PROOF: The same approximations mentioned in the proof of Lemma 2 are needed here. ■ Now we are in position of proving Theorem 1:

PROOF: Let us divide the observation interval $I = (t_0, t_0 + T)$ in M disjoint cells of length Δ each. M depends on T and Δ so as to satisfy $M\Delta = T$. Each cell is centered at a point t_m , $1 \leq m \leq M$. This creates a lattice of $M \times R$ observation cells, M for each of the R receivers. Let us denote a cell with $I(m, r)$, with the obvious meaning for the indices m and r .

1. The input in interval $I(m, r)$ is given by $\int_{\Delta} \lambda_r(t) dt \simeq \lambda_r(t_m)\Delta$. Let us denote the input in the cell $I(m, r)$ by $\lambda_r(t_m)$, and the set of all inputs by $\underline{\lambda} \triangleq \bigcup_{r=1}^R (\lambda_r(t_1), \dots, \lambda_r(t_M))$.
2. The output is the number of arrivals $n(m, r)$ in $I(m, r)$, and is Poisson distributed with parameter $\lambda_r(t_m)\Delta$. For M large enough, and a fixed t_k , the number of arrivals is Bernoulli distributed along the receivers. Let us define $n(m, r)$ as the number of arrivals in the cell $I(m, r)$, and $\underline{n} \triangleq \bigcup_{r=1}^R (n(1, r), \dots, n(M, r))$.

The mutual information between the input intensities $\lambda(t)$ and the arrivals \underline{n} is now given by:

$$I(\lambda(t); \underline{n}) = \lim_{M \rightarrow +\infty} I\left(\bigcup_{r=1}^R \lambda_r(t_1), \dots, \lambda_r(t_M); \bigcup_{r=1}^R n(r, 1), \dots, n(r, M)\right) \quad (\text{A.3})$$

$$= \lim_{M \rightarrow +\infty} I(\underline{\lambda}; \underline{n}) = \lim_{M \rightarrow +\infty} H(\underline{n}) - H(\underline{n}|\underline{\lambda}) \quad (\text{A.4})$$

Let us start with the conditional entropy $H(\underline{n}|\underline{\lambda})$. For a given intensity λ , the outputs are conditionally independent. We apply Lemma 2 to each of these terms:

$$H(\underline{n}|\underline{\lambda}) = \sum_{r=1}^R \sum_{m=1}^M E_{\lambda_r(t_m)} H(n(m, r)|\lambda_r(t_m)) \quad (\text{A.5})$$

$$= \sum_{r=1}^R \sum_{m=1}^M \left(E\{\lambda_r(t_m)\} \Delta - E\{\lambda_r(t_m)\} \psi(\Delta) \right) - \sum_{r=1}^R \sum_{m=1}^M \int_{\lambda_r(t_m)} p(\lambda_r(t_m)\Delta) \psi(\lambda_r(t_m)) d\lambda_r(t_m) \quad (\text{A.6})$$

Let us now go back to the term $H(\underline{n})$. We now define the past as the set of all cells coming before $I(m, r)$, and denote it with $I_{\alpha}(m, r)$ ¹. For the time being we leave the ordering arbitrary.

¹Any ordering would be valid, and that natural need not be followed.

We can decompose it as a sum:

$$H(\underline{n}) = \sum_{r=1}^R \sum_{m=1}^M E_{n(I), I \in I_\alpha(m,r)} H(n(m,r) | n(I)) \quad (\text{A.7})$$

From the memoryless property of the Poisson process, the sequence $(n(I), I \in I_\alpha(m,r)) \rightarrow \lambda_r(t_m) \rightarrow n(m,r)$ forms a Markov chain, so that we can define an a posteriori probability $p_\alpha(\lambda_r(t_m) | n(I))^2$:

$$p_\alpha(\lambda_r(t_m) | n(I)) \triangleq p(n(I) | \lambda_r(t_m)); \quad I \in I_\alpha(m,r) \quad (\text{A.8})$$

We now define an equivalent $\hat{\lambda}_r(t_m)$, as the expected value of the estimate of $\lambda_r(t_m)$ from the past, and whose density is given by $p_\alpha(\lambda_r(t_m) | n(I))p(\lambda_r(t_m))$:

$$\hat{\lambda}_r(t_m) = \int_{\lambda_r(t_m)} p(\lambda_r(t_m)) p_\alpha(\lambda_r(t_m) | n(I)) \lambda_r(t_m) \Delta d\lambda_r(t_m) \quad (\text{A.9})$$

We now invoke Lemma 3 to calculate the value of $H(n(m,r) | n(I))$:

$$H(n(m,r) | n(I)) = \hat{\lambda}_r(t_m) - \psi(\hat{\lambda}_r(t_m)) \quad (\text{A.10})$$

This allows us to rewrite Eq. (A.7) in a more convenient form:

$$H(\underline{n}) = \sum_{r=1}^R \sum_{m=1}^M E_{n(I), I \in I_\alpha(m,r)} H(n(m,r) | n(I)) \quad (\text{A.11})$$

$$\begin{aligned} &= \sum_{r=1}^R \sum_{m=1}^M E_{n(I), I \in I_\alpha(m,r)} \left(\hat{\lambda}_r(t_m) \Delta - \hat{\lambda}_r(t_m) \psi(\Delta) \right) \\ &\quad - \sum_{r=1}^R \sum_{m=1}^M E_{n(I), I \in I_\alpha(m,r)} \psi(\hat{\lambda}_r(t_m)) \Delta \end{aligned} \quad (\text{A.12})$$

We now exploit the fact that by construction,

$$E_{n(I), I \in I_\alpha(m,r)} \hat{\lambda}_r(t_m) = \quad (\text{A.13})$$

$$= E_{n(I), I \in I_\alpha(m,r)} \int_{\lambda_r(t_m)} p(\lambda_r(t_m)) p_\alpha(\lambda_r(t_m) | n(I)) \lambda_r(t_m) d\lambda_r(t_m) \quad (\text{A.14})$$

$$= \int_{\lambda_r(t_m)} \left(E_{n(I), I \in I_\alpha(m,r)} p_\alpha(\lambda_r(t_m) | n(I)) \right) p(\lambda_r(t_m)) \lambda_r(t_m) d\lambda_r(t_m) \quad (\text{A.15})$$

$$= \int_{\lambda_r(t_m)} 1 \cdot p(\lambda_r(t_m)) \lambda_r(t_m) d\lambda_r(t_m) = E\{\lambda_r(t_m)\}. \quad (\text{A.16})$$

Common terms vanish in Eqs. (A.6) and (A.12), and the mutual information is given by:

$$I(\underline{\lambda}; \underline{n}) = \sum_{r=1}^R \sum_{m=1}^M E_{\lambda_r(t_m)} \left\{ \Delta \psi(\lambda_r(t_m)) \right\} - \sum_{r=1}^R \sum_{m=1}^M E_{n(I), I \in I_\alpha(m,r)} \left\{ \Delta \psi(\hat{\lambda}_r(t_m)) \right\}, \quad (\text{A.17})$$

²Note that if there is no statistical correlation among $\lambda_r(t_m)$, the past will not give extra information on the present, and the a posteriori probability will be irrelevant.

where the last equality follows from the same reasoning as in Eqs. (A.13)–(A.16). Finally, in the limit $M \rightarrow +\infty$, the summation becomes an integral, and we obtain

$$I(\lambda(t); \underline{\tau}) = \sum_{r=1}^R \int_t^R E_{\lambda_r(t)} \left\{ \lambda_r(t) \log(\lambda_r(t)) \right\} dt - \sum_{r=1}^R \int_t^R E_{\underline{\tau}(I), I_\alpha(t,r)} \left\{ \hat{\lambda}_r(t) \log(\hat{\lambda}_r(t)) \right\} dt. \quad (\text{A.18})$$

$I_\alpha(t, r)$ is the continuous-time ordering derived from the discrete equivalent $I_\alpha(m, r)$. ■

APPENDIX B

THEOREM 4: For a given channel intensity $\lambda(t)$, defined in a time interval $(t_0, t_0 + T)$, the entropy of the observed sequence of arrival times $\underline{\tau}$ is given by:

$$h(\underline{\tau}|\lambda(t)) = \int_{t_0}^{t_0+T} \lambda(t) dt - \int_{t_0}^{t_0+T} \lambda(t) \log \lambda(t) dt. \quad (\text{B.1})$$

PROOF: Starting with the definition of entropy, and using the well-known expression for the probability $\Pr(\underline{\tau}|\lambda(t)) = e^{-\Lambda} \prod_{i=1}^k \lambda(\tau_i)$, we get:

$$h(\underline{\tau}|\lambda(t)) = - \sum_{k=0}^{+\infty} \int_{\underline{\tau}} e^{-\Lambda} \prod_{i=1}^k \lambda(\tau_i) \log \left(e^{-\Lambda} \prod_{i=1}^k \lambda(\tau_i) \right) d\underline{\tau}, \quad (\text{B.2})$$

where we group the terms in the sum so that each $\underline{\tau}$ consists of k arrivals. Let this contribution to the entropy be denoted by h_k . By symmetry, the partition of the interval $(t_0, t_0 + \Delta)^k$ is such that it covers an area exactly $1/k!$ of the total area of the original interval. We thus obtain

$$\begin{aligned} h_k(\underline{\tau}|\lambda(t)) &= -e^{-\Lambda} \int_{\tau_1} \cdots \int_{\tau_k > \tau_{k-1}} \lambda(\tau_1) \cdots \lambda(\tau_k) \left(-\Lambda + \sum_{i=1}^k \log \lambda(\tau_i) \right) d\tau_1 \cdots d\tau_k \\ &= -e^{-\Lambda} \frac{1}{k!} \int_{\tau_1} \cdots \int_{\tau_k} \lambda(\tau_1) \cdots \lambda(\tau_k) \left(-\Lambda + \sum_{i=1}^k \log \lambda(\tau_i) \right) d\tau_1 \cdots d\tau_k. \end{aligned} \quad (\text{B.3})$$

After some more calculations, we obtain

$$\begin{aligned} h_k &= e^{-\Lambda} \frac{1}{k!} \Lambda \left(\int_{\tau} \lambda(\tau) d\tau \right)^k - e^{-\Lambda} \frac{1}{k!} \sum_{i=1}^k \int_{\tau_1} \cdots \int_{\tau_k} \log \lambda(\tau_i) \lambda(\tau_1) \cdots \lambda(\tau_k) d\tau_1 \cdots d\tau_k \\ &= e^{-\Lambda} \frac{1}{k!} \Lambda^{k+1} - e^{-\Lambda} \frac{1}{k!} k \left(\int_{\tau} \lambda(\tau) d\tau \right)^{k-1} \left(\int_{\tau} \lambda(\tau) \log \lambda(\tau) d\tau \right) \end{aligned} \quad (\text{B.4})$$

$$= e^{-\Lambda} \frac{1}{k!} \Lambda^{k+1} - e^{-\Lambda} \frac{1}{(k-1)!} \Lambda^{k-1} \Lambda_L. \quad (\text{B.5})$$

where $\Lambda = \int_{\tau} \lambda(\tau) d\tau$ and $\Lambda_L \triangleq \int_{\tau} \lambda(\tau) \log \lambda(\tau) d\tau$. Putting all terms together:

$$\begin{aligned} h(\underline{\tau}|\lambda(t)) &= \sum_{k=0}^{+\infty} h_k(\underline{\tau}|\lambda(t)) = \sum_{k=0}^{+\infty} e^{-\Lambda} \frac{1}{k!} \Lambda^k - \sum_{k=1}^{+\infty} e^{-\Lambda} \frac{1}{(k-1)!} \Lambda^{k-1} \Lambda_L \\ &= \Lambda e^{-\Lambda} e^{\Lambda} - \Lambda_L e^{-\Lambda} e^{\Lambda} = \Lambda - \Lambda_L. \end{aligned} \quad (\text{B.6})$$

■

APPENDIX C

PROPOSITION 5: Let the signal intensity $\lambda(t)$ be piecewise-constant, with the points of change (discontinuity) denoted by $t_i, i = 0, \dots, \ell$, ℓ may be infinite for a countable number of discontinuities. Each interval is then of the form $[t_i, t_{i+1})$; let us define $\Delta t_i \triangleq t_{i+1} - t_i$. Let \underline{k} denote a vector with the number of arrivals at each interval, and $\underline{\tau}$ the corresponding arrival times. The probabilities $\Pr(\underline{\tau}|\lambda(t))$ and $\Pr(\underline{k}|\lambda(t))$ are linked via the following equation:

$$\Pr(\underline{\tau}|\lambda(t)) = \Pr(\underline{k}|\lambda(t)) \prod_{i=0}^{\ell} \frac{k_i!}{\Delta t_i^{k_i}}. \quad (\text{C.1})$$

PROOF: The signals $\lambda(t)$ are constant in each interval $[t_i, t_{i+1})$, so that the $\lambda(\tau_j)$ is a function of the interval number only. If we now integrate over all possible arrival sequences compatible with a given vector \underline{k} , we obtain

$$\Pr(\underline{k}|\lambda(t)) = \int_{\underline{\tau}} e^{-\Lambda} \prod_{i=1}^{\ell} \prod_{j=1}^{k_i} \lambda(\tau_j) d\underline{\tau} = e^{-\Lambda} \prod_{i=1}^{\ell} \frac{\prod_{j=1}^{k_i} \lambda(\tau_j)(\Delta t_i)}{k_i!}. \quad (\text{C.2})$$

Using the constantness property, we obtain the desired equation by grouping terms. ■

PROPOSITION 6: Under the assumptions of Proposition 5 the entropies $h(\underline{\tau})$ and $H(\underline{k})$ are related via the following equation:

$$h(\underline{\tau}) = - \sum_{\underline{k}} \Pr(\underline{k}) \log \left(\Pr(\underline{k}) \prod_{i=0}^{\ell} \frac{k_i!}{\Delta t_i^{k_i}} \right) \quad (\text{C.3})$$

$$= H(\underline{k}) - \sum_{\underline{k}} \Pr(\underline{k}) \sum_{i=0}^{\ell} \log \frac{k_i!}{\Delta t_i^{k_i}}. \quad (\text{C.4})$$

PROOF: Note that the extra factor in Eq. (C.1) does not depend on the signal $\lambda(t)$, but only on the instants t_i , so that the same constant of proportionality holds for total probabilities $\Pr(\underline{\tau}) = \sum_{\lambda} \Pr(\underline{\tau}|\lambda(t))$.

We can again decompose the integration over $\underline{\tau}$ in terms for fixed \underline{k} . For fixed \underline{k} , all the compatible terms $\tau^{(\underline{k})}$ do not depend on time, and the integral of $\Pr(\tau^{(\underline{k})}) \log \Pr(\tau^{(\underline{k})})$ is very easy, that of a constant. We now exploit that this integral gives the same proportionality term as Proposition 5, and simple calculations yield now Eq. (C.4). ■

REFERENCES

- [1] Y. Kabanov, "The capacity of a channel of the Poisson type," *Theory of Probability and Applications*, vol. 23, pp. 143–147, 1978.
- [2] M. H. A. Davis, "Capacity and cutoff rate for Poisson-type channels," *IEEE Trans. Inform. Theory*, vol. 26, pp. 710–714, November 1980.
- [3] A. D. Wyner, "Capacity and error exponent for the direct detection photon channel - part I," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1449–1461, November 1988.
- [4] A. D. Wyner, "Capacity and error exponent for the direct detection photon channel - part II," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1462–1471, November 1988.
- [5] A. Lapidoth and S. M. Moser, "Bounds on the capacity of the discrete-time Poisson channel," in *Proceedings of the 41st Allerton Conf. on Communication, Control, and Computing*, October 2003.

QSPACE PROJECT: QUANTUM CRYPTOGRAPHY IN SPACE

Cesare Barbieri¹, Gianfranco Cariolaro², Tommaso Occhipinti²,
Claudio Pernechele³, Fabrizio Tamburini^{1,2}, and Paolo Villoresi²

¹*Dept. of Astronomy, University of Padova, vicolo dell'Osservatorio 2, I-35122 Padova, Italy;*

²*Department of Information Engineering, University of Padova, via Gradenigo 6/B,
I-35131 Padova, Italy;*

³*INAF, Cagliari Observatory, Strada 54, Poggio dei Pini I-09012 Capoterra (CA), Italy.*

Abstract: The purpose of this project is to improve the techniques of Quantum Cryptography, to realize a Quantum Key Distribution (QKD) in free space with an orbiting satellite using nowadays technology. With this experiment we characterize the properties of a single photon communication channel from an orbiting satellite in space to a ground based station. We used the facilities of the ASI laser ranging station MLRO (Matera) and the satellite for geodesy Lageos I, equipped with corner-cube retroreflectors, to simulate a single photon transmission from an orbiting satellite.

Key words: optical communication; quantum cryptography; quantum communication; space technology.

1. INTRODUCTION

Quantum mechanics provides powerful tools that form one of the cornerstones of scientific progress, and which are indispensable for nowadays technology. The most important areas where the applications of Quantum mechanics will be crucial in the next future are the new developments in modern communication and information-processing technologies, namely Quantum Communication, Quantum Teleportation with entangled states and Quantum Computation. Quantum Cryptography is the most promising application of Quantum Communication in every day's life of the next future, together with Quantum Teleportation [1–4]. Here the fundamental properties of quantum mechanics are used to enhance the power and potential of today's communication and

security systems, providing a secure alternative to the conventional encryption methods that will resist also quantum computer attacks. While Quantum Teleportation and Quantum Computation mainly utilize entanglement between two or more particles, Quantum cryptography can also be performed even with single quantum particles.

Single photon communication

Single photon communication allows an ideally secure generation and distribution of a cryptographic key between two distant parties. Quantum Key Distribution (QKD) in fact uses the fundamental laws of quantum mechanics that describe the transmission of quantum states of the light [5–7]. The distribution of the cryptographic key must be secure against the attack of a third party that tries to acquire information with an eavesdropping technique. The vital advantage quantum mechanics provides lies in the impossibility that an eavesdropper (Eve) can intercept the secret key, made up of individual quanta, without revealing her presence to Alice, the sender and Bob, the receiver, since such interception unavoidably alters and destroys the quantum state of the photon. An attack may be made by Eve who secretly attempts to determine the key intercepting the travelling photons from Alice to Bob. By performing a sequence of measurements on these quanta, Alice and Bob determine the key they will use to encrypt their message. This aspect derives directly from the laws of quantum mechanics and it is also known as “No-cloning theorem”, which states that it is not possible to duplicate a generic single quantum state without measuring it, thus without perturbing it in an irreversible way. The measurement on a quantum state in fact has not the meaning of revealing information coded in the quantum state, as it happens for the classical case. The sender Alice builds the cryptographic key with a sequence of single quanta prepared in different complementary quantum states. The easiest way is the use of the polarization states associated to single photons. The sender Alice randomly prepares the state of a photon and sends it to the receiver Bob. He then establishes the cryptographic key by independently performing a sequence of random polarization measurements on the photons. Both Alice and Bob will independently generate two random sequences of “0”s and “1”s corresponding to the different outcomes of their polarization measurements. The cross-correlation of the random sequences and the protocol chosen by Alice and Bob will generate the quantum key. The two major protocols are those by Bennett and Brassard [8] and Bennett [9] (see [10] for a review). The application of space and astronomical technologies to Quantum Communication will make possible the realization of a future quantum cryptography-based network of Satellites and ground stations which will guarantee a completely secure,

global, long-range communication system: a novel field which will disclose entirely new ways of exchanging information between distant observers.

2. THE Q-SPACE PROJECT

The theoretical properties of quantum information and the feasibility of quantum communication in practical situations have been already elucidated by many experiments carried out in laboratories on the ground.

Our experiment points out the fundamental advantages to be obtained by using a Space system, advantages that could lead to a deeper understanding of the theory and to novel utilisation. The aim of this experiment is to realize the first quantum communication from satellite to ground with single photons. This link is realized with the Matera Laser Ranging Observatory (MLRO) in conjunction with an existing retroreflecting satellite such as Lageos [11]. A laser beam, collimated by MLRO, will illuminate the retroreflectors onboard Lageos and simulate the transmission of single photons from satellite to ground. After the retroreflection, the detection and characterization of the quantum state associated to each photon through MLRO itself will simulate the QKD process. In this experiment we simulate Alice, the sender, located on the satellite and Bob, the receiver, in the ground station.

2.1 Description of the experimental setup

2.1.1 Properties of MLRO laser ranging system. The laser ranging station is equipped with a 1.5 meter mirror telescope with astronomical quality optics, Cassegrain configuration $f/212$, long Coudé. The beam divergence is "diffraction limited" and can be tuned in a continuous way from around 1" to 20". The alt-azimuth mount is capable of a tracking velocity of 20 deg/sec in azimuth and 5 deg/sec in elevation, with a tracking accuracy of 1 arcsec RMS. The MLRO laser is an active hybrid ND:YAG configured to emit 40 ps fast pulses in the wavelength of 532 nm with an impulse of 100 mJ/pulse in the monochromatic setup. The averaged estimated number of photons per pulse is $\sim 5 \times 10^{17}$. The clock of the laser system is 10 Hz, with a range timing accuracy better than 2 ns, which is too slow to realize a quantum key with single photons from the satellite. This immediately requires, that the pulse rate of the laser is increased by many orders of magnitude. At 10 Hz pulse rate, it would require 30 days to capture 1 single event for the best case.

2.1.2 Properties of the retroreflecting targets. Here the ground based station MLRO acts as photon source for the orbiting Alice. To simulate Alice on the satellite, we will use mainly the Laser GEodynamics Satellite 1 LA-GEOS 1 (ASI/NASA), a spherical-shape satellite for geodesy equipped with corner-cube retroreflectors, diameter 60 cm, with perigee height of 5900 km.

The satellite is equipped with 426 retroreflectors built in such a way to send most of the signal back to the same direction of the incident light. Each retroreflector is essentially a cylindrical piece of glass having a 3.8 cm in diameter and a 3-surface reflecting corner.

2.1.3 The quantum transceiver. We use the laser ranging facility of MLRO to center the satellite with high precision and its optical transmission line for our optical transmission/receiver device, the Quantum transceiver (QT).

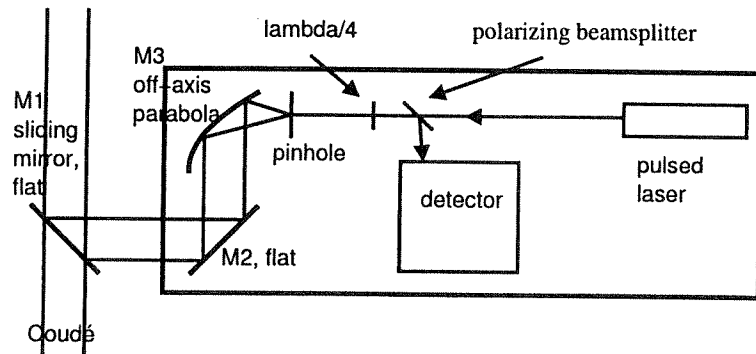


Figure 1. Schematic of the Quantum transceiver.

QT is equipped with a weaker, but higher repetition rate laser, able to realize a quantum key distribution. The laser is a Nd:YAG laser with a passive Q-switching and integrated second harmonic generator, centered at 532 nm, with repetition rate of 17 kHz, which emits about 10^{12} photons per shot. The transmission and receiving line have the same optical paths, and use the polarization of light to discriminate the outgoing and incoming signals. The transmission is realized by opportunely polarized collimated pulses, focalized onto a pinhole, and expanded to the exit pupil diameter of the MLRO telescope by the off-axis parabola. After the retroreflection from the satellite, the beam passes again through a pinhole is recollimated with a lens, and directed by the polarizing beamsplitter to the detector, a Si-APD photon counter. To reduce the noise due to the light background (atmosphere, celestial sources, environmental, etc.) we choose a very small field of view, centered on the satellite position, with radius 1.4 to 2.2 arcsec. An additional improvement is given by the insertion of a narrowband filter with 0.15 nm of FWHM in the optical path to the detector and the time-tagging, obtained by setting up a set of time-windows, where to look for a positive detection by calculating the time of flight of laser pulse. This would allow us to label each possible photon reflected from the satellite, even if embedded in the background light, with a certain, finite, probability of success.

3. CATCHING THE PHOTON

3.1 Orbital fit and the link budget equation

The time of flight of the photons retroreflected by the satellite is varying in time, during the motion of the satellite itself. To determine exactly the set of coincidences for the time-tagging, we performed a polynomial fit obtaining only a few ns RMS difference between measured and fitted range points.

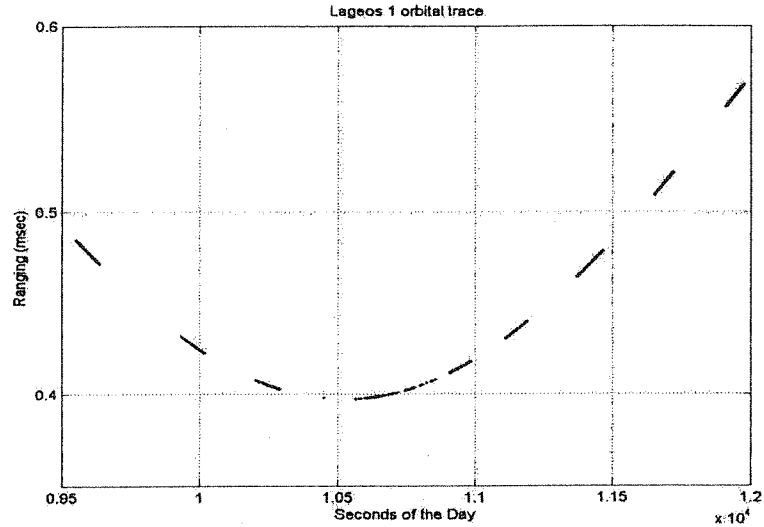


Figure 2. LAGEOS 1 : time of flight of a photon (from 40 to 58 ns) vs time.

A better determination of the time of flight can be obtained with Geodyn II (NASA/GSFC) program [5], with an actual error of 5-6 mm RMS in the position of the satellite. The post fit radial residuals for a good pass observed by MLRO is less than 1 cm RMS (often less than 5 mm RMS) for all targets. We now consider how to achieve single photon transmission from the satellite and single photon reception at the MLRO station by calculating the energy budget of the retroreflected light to choose the right energy to be transmitted. The returned energy is given by the link budget equation, which gives the number of reflected photons and then the number of photoelectrons, depending on different situations during the observation.

$$N_{phe} = \eta_q E_T \frac{\lambda}{hc} \eta_T G_T \sigma_{sat} \left(\frac{1}{4\pi R^2} \right)^2 A_T \eta_R T_A^2 T_c^2$$

here η_q is the detector quantum Efficiency, η_T the transmit path efficiency, η_R receive-path efficiency, A_T the receiving aperture area of the telescope, T_A the atmospheric transmission, T_c cloud transmission, E_T the laser energy pulse,

σ_{sat} the satellite backscattering cross section and G_T the transmit gain. A quite comprehensive description of the link budget calculation is given by Degnan [12]. The link budget is function of R^{-4} , R being the distance of the satellite from the earth (another way of expressing it, is by using the square of the beam divergence D). The main limiting factor of the efficiency is the size of the retroreflectors, which are only 3.8 cm in diameter. Furthermore, since the satellite is not stabilized, the retroreflectors must have some beam spreading. Taking now into account the effective area and the diffraction effects of the Lageos retroreflectors and of MLRO telescope, the total efficiency would then be about 10^{-16} – 10^{-13} , i.e., 0.0001–0.1 retroreflected photons per pulse.

3.2 Atmospheric seeing problems

The Earth's turbulent atmosphere causes stars to "twinkle" and their intensity undergo rapid fluctuations. This also happens for the signal sent by Alice on the satellite.

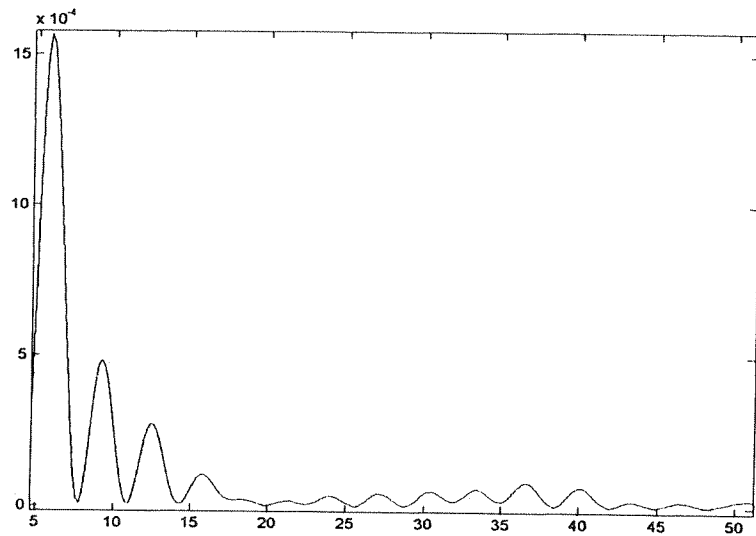


Figure 3. Power Spectrum of Arcturus from 3 to 55 Hz.

The measured probability distributions for the arrival of the photons in time arise from a combination of the atmospheric fluctuations with the Poisson distribution of the photon counts. Previous studies on the analysis of atmospheric intensity scintillation of stars [13] show that the time distribution of the photon counts is quite complicated, which cannot easily fit neither with a Poissonian nor a Lognormal distribution. We characterized the effects due to the seeing, and the eventual loss in the transmission, by measuring the intensity of some test stars with our transceiver. In our power spectrum analysis of the signal

of Arcturus, α Bootis, we find two peaks below 10 Hz, which can be ascribed to the guiding of the telescope. The effects of seeing, due to the atmospheric turbulence tilt of the wavefront, are in the peaks seen at higher frequencies.

3.3 Acquisition from ground targets

The calibration of our instrument was obtained by measuring the return signal from a selected ground target (corner cube), located at 42.25 m, i.e., with a time of flight of 150.92 ns for each photon. We obtained 100% of returns. In Fig. 4 we report the log of the number of the returned signal counts from 50000 pulses vs. the difference between the expected time of flight and the actual arrival time within 10 ns.

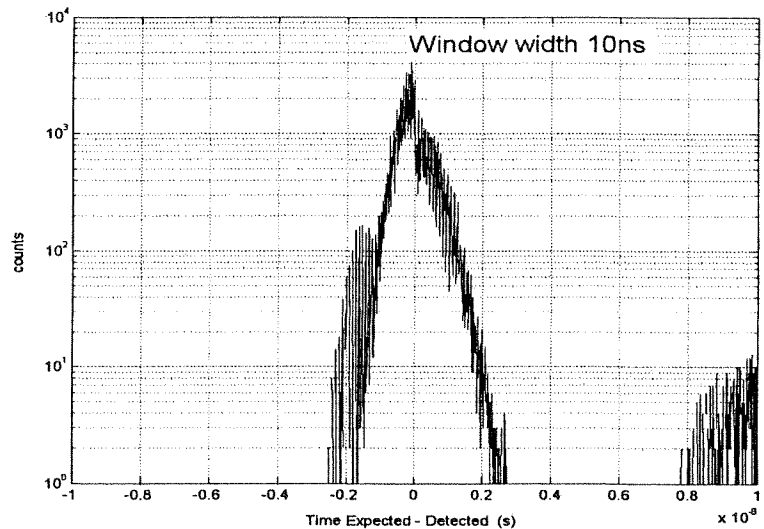


Figure 4. Logplot of the measured returns from a fixed target and difference between the time of flight and the detected time.

The main central peak contains almost all the returns and its width is caused by the non perfect regularity in the sequence of the laser pulses due to the Q-switching mechanism of the laser; the other peak on the right is negligible, and can be caused by electronics bouncing. The data acquisition and analysis from orbiting satellites are now in progress.

4. CONCLUSIONS

The first simple experiments made during the realization of the Matera-LAGEOS link, show that with nowadays technology the realization of a quantum cryptography link is feasible, without requiring much extra equipment, which can then serve as the basis for future large scale projects using dedi-

cated space systems. This will be probably the first in the world experiment of such kind. This application represents the “quantum leap” that will transform a classical optical communication channel in a quantum channel, where it is possible to implement secure communication protocols based on Quantum Cryptography.

REFERENCES

- [1] D. Bouwmeester, J.-W. Pan, M. Daniell, H. Weinfurter, M. Zukowski, and A. Zeilinger, “Reply: A posteriori teleportation,” *Nature*, vol. 394, no. 6696, p. 841, 1998.
- [2] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, “Violation of Bell’s inequality under strict Einstein locality conditions,” *Phys. Rev. Lett.*, vol. 81, no. 23, pp. 5039–5043, 7 Dec. 1998.
- [3] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, “Quantum cryptography with entangled photons,” *Phys. Rev. Lett.*, vol. 84, no. 20, pp. 4729–4732, May 2000.
- [4] M. Aspelmeyer, H. R. Böhm, T. Gyatso, T. Jennewein, R. Kaltenbaeck, M. Lindenthal, G. Molina-Terriza, A. Poppe, K. Resch, M. Taraba, R. Ursin, P. Walther, A. Zeilinger, “Long-distance free-space distribution of quantum entanglement,” *Science*, vol. 301, no. 5633, pp. 621–623, Aug. 2003.
- [5] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, “Practical free-space quantum key distribution over 1 km,” *Phys. Rev. Lett.*, vol. 81, no. 15, pp. 3283–3286, Oct. 1998.
- [6] W. T. Buttler, R. J. Hughes, P. G. Kwiat, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, “Free-space quantum-key distribution,” *Phys. Rev. A*, vol. 57, pp. 2379–2382, 1998.
- [7] J. Cerne, M. Grayson, D. C. Schmadel, G. S. Jenkins, H. D. Drew, R. Hughes, A. Dabkowski, J. S. Preston, and P.-J. Kung, “Infrared Hall effect in high- T_c superconductors: Evidence for non-Fermi-liquid Hall scattering,” *Phys. Rev. Lett.*, vol. 84, no. 15, pp. 3418–3421, Apr. 2000.
- [8] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *Proc. IEEE International Conference on Computers, Systems, and Signal Processing*, (Bangalore, India), pp. 175–179, Dec. 1984.
- [9] C. H. Bennett, “Quantum cryptography using any two nonorthogonal states,” *Phys. Rev. Lett.*, vol. 68, no. 21, pp. 3121–3124, 25 May 1992.
- [10] D. Bouwmeester, A. Ekert, and A. Zeilinger, *The Physics of Quantum Information*, Springer, 2000.
- [11] See for further information <http://ilrs.gsfc.nasa.gov/>
- [12] J. J. Degnan, “Millimeter accuracy satellite laser ranging: A review,” in *Contributions of Space Geodesy to Geodynamics: Technology* (D. E. Smith and D. L. Turcotte, eds.), AGU Geodynamics Series, vol. 25, pp. 133–162, 1993.
- [13] D. Dravins, L. Lindegren, E. Mezey, and A. T. Young, “Atmospheric intensity scintillation of stars,” *PASP*, vol. 109, pp. 173–207, 1997.

QUANTUM-AIDED CLASSICAL CRYPTOGRAPHY WITH A MOVING TARGET

Fabrizio Tamburini^{1,3}, Sante Andreoli², and Tommaso Occhipinti^{1,3}

¹*Dept. of Astronomy, University of Padova, vicolo dell'Osservatorio 2, I-35122 Padova, Italy.*

²*Magneti Marelli Holding S.p.A., Motorsport.*

³*Department of Information Engineering, University of Padova, via Gradenigo 6/B, I-35131, Padova, Italy.*

Abstract: We propose an encryption method obtained combining low-light optical communication, in the limit of quantum key distribution (QKD) techniques, and classical cryptography with pre-shared key. We present a toy-application to the telemetric data transmission Formula 1 racing.

Key words: optical communication; secure communication; cryptography; quantum cryptography.

1. INTRODUCTION

The recent method proposed to create and distribute securely a quantum encryption key to send secure messages takes its vital inspiration from the basic laws of quantum mechanics. Quantum cryptography started with the studies by Bennett and Brassard in 1980s and by Bennett in 1992 [1, 2] as a new method for generating and distributing secure cryptographic keys using the properties of Quantum Mechanics. In contrast to existing methods of classical key distribution (CKD), quantum key distribution, QKD bases its security on the laws of nature. The impossibility of cloning or measuring a quantum state without inducing an irreversible collapse of its wavefunction ensures the build-up of a secure cryptographic key distribution between two parties. For a review see e.g. [3]. Similar experiments [4, 5] illustrated the feasibility of quantum encryption in practical situations. Free-space QKD was first realized [6, 7] over a small distance of 32 cm only with a point-to-point table top optical path, and recently improved in atmospheric transmission distances of 75 m [8] in daylight and 1 km [9] in nighttime over outdoor folded paths, where the quanta

of light were sent to a mirror and back to the detector. A daylight quantum key distribution had been realized over a distance of 1.6 km by Buttler et al. [5]. Recently Aspelmeyer et al. realized a quantum key distribution over the Danube using entangled photons [10]. Several groups have also demonstrated QKD over multi-kilometer distances of optical fiber [11–17] and recently realized a version of the experiment “in the real world”, in which Alice and Bob were connected with 1.45 km of optical fiber sharing entangled photons. The average raw key bit rate was found to be about 80 bits/s after error correction and privacy amplification. idQuantique, MagiQ technologies and NEC realized commercial applications of secure quantum key distribution [18–20]. MagiQ technologies guarantee, for example, a fast-generating quantum key rate of 10 keys per second. The field is now sufficiently mature to be commercially implemented and to be a tool in fundamental research beyond the foundations of quantum mechanics and basic physics [21, 22].

2. QKD TO UPDATE A “MOTHER KEY”

In this paper we suggest a simple procedure to aid the classical cryptographic methods with Quantum Cryptography, when the environmental conditions and/or the requirements of obtaining a long key in a short time strongly play against QKD. This procedure will increase, time-by-time, with the one-time-pad methods of Quantum Cryptography, the global security of the scheme. This method was studied to improve the security of bi-directional telemetry of race cars in view of possible, future, quantum computer attacks.

A classical cryptographic scheme can be reduced to three main quantities: m the message, k the key and c the code, with the corresponding random variables M , K and C that describe their statistical behaviours. The encoding $C = \text{Code}(M, K)$ and the decoding $M = \text{Dec}(C, K)$ are suitable deterministic processes which are described by a set of instructions τ that require a computational effort that depends both on the length of the cryptographic key and on the chosen protocol. Even if modern classical encryption protocols, based on the computational complexity of their encoding algorithms, still resist to the attacks made with nowadays technology, they will become vulnerable in the next future to the attacks of quantum computers, e.g. with Shor’s algorithm (for a review, see [23]).

This problem will be avoided with a fast-generating QKD scheme that will change the key with a rate much faster than the computational time needed to break the code, without giving enough time to the cracker to get the encoded information. In environmental conditions with high bit error rate the application of this procedure will become more and more difficult giving more chances to the cracker to break the code.

We propose a simple thought experiment, in a noisy environment, as alternative to realize a secure fast encryption in real time using an ancillary key k' obtained via QKD, to update a classical pre-shared cryptographic key k with a simple change, such as bit shift or another more complex cyphertext method. k , the *mother cryptographic key*, can be previously securely loaded in a secure environment.

The updating process of k is a simple encryption of k itself with k' , and the new key thus obtained, $k'' = \text{Cod}(K, K')$, s.t. $\text{length}(k'') = \text{length}(k)$, is used to encrypt new messages. k' has a randomly variable length that depends on the efficiency of the QKD process: $\text{length}(k') \leq \text{length}(k)$.

This method will be less and less useful in the limit of the ideal case, i.e. when $\text{length}(k') = \text{length}(k)$. This satisfies the prescriptions of a perfect secure scheme for the encryption of k , and the space of obtainable new keys is the space of the messages $M = K$, $H = K'$ and the space of generated codes is given by the new key k'' . In this limit we have the classical, safest, encryption procedure: the key has the same length as the message to be sent but it is also the case in which the methods of QKD are fully applicable.

In the worst case, if a run of the QKD updating process does not have success and $k' = \emptyset$, is the null set, the map Cod becomes the identity map and $k'' = k$, ensuring that the message will be in any case encrypted by the previous key.

The two encryption methods, classical and quantum, are combined together to increase the security of the transmission. The intrinsic weakness of the classical key distribution between two distant parties, can be aided by the impossibility of a third-party eavesdropping with QKD, while the failures due to the non-optimal environmental conditions which usually play against QKD in the building quickly a key in real time, are supported by previously selected cryptograms and CKD with a pre-shared key.

A possible application is the realization of a secure communication of telemetric data between two parties in relative motion. An example is a key exchange between an airplane and a ground station or between a race car and the Box. Real-time telemetric data transmission needs in fact an immediate and secure encoding process, which cannot be easily guaranteed at the moment using only QKD.

3. TOY-APPLICATION IN F1 RACING

Here we studied the possible application of this method to encrypt the telemetry of a race car during a Grand Prix. Alice is located at the Box, while Bob is driving the car. Alice and Bob initially share a secret classical cryptographic key k with length N exchanged before the race, and choose a classical protocol to realize a secure communication such as DES, 3DES or AES. The Quantum

Cryptographic Key k' obtained by exchanging single-photon pulses from the box line to the car during a passage close to the box has the purpose to give to the on-board computer only information to start cyphertext methods on the mother Key.

The immediate advantage is that with this method we can, in principle, realize quite a secure encryption only adopting a mother key 256 bit long, reducing the additional computational requirements to the onboard electronics.

To realize a single-photon QKD from the box to the car in a race track we also have to satisfy some precise requirements:

1. Strong weight constrains: no mechanically moving parts to realize polarization swapping no laser devices mounted into the car.
2. The usual procedure of Quantum key authentication utilizes the resources onboard the car and is convenient to embed them inside the telemetric data.
3. Data transmission must be classically encrypted even in the case of QKD failure.
4. The laser must works in non-visible light at 1550nm, and this procedure is safe for the driver: each pulse is in fact made with a very faint source, ideally from 0.1 to 1 photon per shot as required by QKD.

In the simplest case, the car is equipped with a set of passive detectors device realized with single-photon detectors, polarizers and fiber-injection optics as in the figure. The noise due to the environmental light is screened by a narrowband filter centred at the laser's wavelength of about 1550 nm. Each of the polarizers has different orientations, according with the chosen QKD protocol.

During each passage Alice tracks the car and tells Bob via radio to switch on the electronic control that will activate each of its detectors in a random sequence, which will realize Bob's polarization swapping. Alice sends a random sequence of polarized photon pulses. Alice and Bob will publicly announce their keys via telemetry and will decide whether to encrypt k .

With a commercial LiNbO₃ modulator, Alice can produce ideally a random sequence of polarization swapping with a clock rate up to the GHz rate. Previous experiments showed a clock rate up to 1-MHz [5] for daylight QKD.

In the simplest case, the tracking could be realized by a fixed direction beam-expander, and the car, passing through the region illuminated by Alice's laser would capture some photons to realize the quantum key. With an angular beam width of 0.5° Bob obtains a laser beam expanded up to 20 cm at about 20 m of distance. This would need a fast and efficient QKD process. In fact, for a car travelling at 100 m/s at a distance of 20 m, the beam crossing time is the order the millisecond, which means that we would need 1 MHz of photon counting independently from its polarization state, to build a 256 bit key at each passage.

With a GHz modulator and a laser attenuation to 0.1–1 photons/pulse (as required by single-photon QKD) the total detection efficiency needed is 1/100. The emission of radiation by the car and the track at that specific wavelength can be considered almost constant within the tracking time.

A further step would be the application of adaptive optics to improve the pointing of Alice’s source to Bob.

We could think to extend this procedure of cryptographic key updating also to the case in which the quantum communication channel is replaced with a faint source of polarized photons, even if low-light optical communication is in principle different from QKD.

4. CONCLUSIONS

We proposed a study of feasibility for a method of mixed quantum and classical cryptography with an application to race car telemetry encryption in real time. This method would guarantee the presence of a cryptographic key for a secure telemetry also when the quantum channel is affected by strong noise. We proposed to extend this procedure also when the distribution of the auxiliary key is realized with low-light optical communication.

ACKNOWLEDGMENTS

We would like to thank Prof. G. Cariolaro for his encouragement, comments and suggestions.

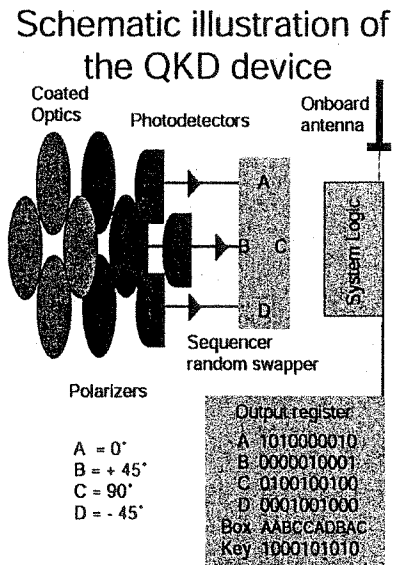


Figure 1. Scheme of the device onboard Bob’s car.

REFERENCES

- [1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE International Conference on Computers, Systems, and Signal Processing*, (Bangalore, India), pp. 175–179, Dec. 1984.
- [2] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, no. 21, pp. 3121–3124, 25 May 1992.
- [3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Jan. 2002.
- [4] R. J. Hughes, W. T. Buttler, P. G. Kwiat, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. Glen Peterson, "Practical quantum cryptography for secure free-space communications," Preprint: quant-ph/9905009, Available: <http://arxiv.org/abs/quant-ph/9905009>, 1999.
- [5] W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. Glen Peterson, "Daylight quantum key distribution over 1.6 km," Preprint: quant-ph/0001088, Available: <http://arxiv.org/abs/quant-ph/0001088>, 2000.
- [6] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. A. Smolin, "Experimental quantum cryptography," in *Advances in Cryptology - EUROCRYPT '90, Workshop on the Theory and Application of Cryptographic Techniques, Aarhus, Denmark, May 21-24, 1990, Proceedings*, (I. B. Damgård, ed.), ser. Lecture Notes in Computer Science, vol. 473, pp. 253–265, Springer, 1991.
- [7] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, "Experimental quantum cryptography," *J. Cryptology*, vol. 5, no. 1, pp. 3–28, 1992.
- [8] B. C. Jacobs and J. D. Franson, "Quantum cryptography in free space," *Opt. Lett.*, vol. 21, no. 22, pp. 1854–1856, 1996.
- [9] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, "Practical free-space quantum key distribution over 1 km," *Phys. Rev. Lett.*, vol. 81, no. 15, pp. 3283–3286, Oct. 1998.
- [10] M. Aspelmeyer, H. R. Böhm, T. Gjatso, T. Jennewein, R. Kaltenbaek, M. Lindenthal, G. Molina-Terriza, A. Poppe, K. Resch, M. Taraba, R. Ursin, P. Walther, A. Zeilinger, "Long-distance free-space distribution of quantum entanglement," *Science*, vol. 301, no. 5633, pp. 621–623, Aug. 2003.
- [11] J. D. Franson, and H. Ilves, "Quantum cryptography using optical fibers," *Appl. Opt.*, vol. 33, no. 14, pp. 2949–2954, 1994.
- [12] C. Marand, and P. D. Townsend, "Quantum key distribution over distances as long as 30 km," *Opt. Lett.*, vol. 20, no. 16, pp. 1695–1697, 1995.
- [13] R. J. Hughes, G. G. Luther, G. L. Morgan, C. G. Peterson, C. M. Simmons, "Quantum cryptography over underground optical fibers," in *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings*, ser. Lecture Notes in Computer Science, vol. 1109, pp. 329–342, Springer, 1996.
- [14] A. Muller, H. Zbinden, and N. Gisin, "Quantum cryptography over 23 km in installed under-lake telecom fibre," *Europhys. Lett.*, vol. 33, no. 5, pp. 335–339, 1996.
- [15] R. J. Hughes, W. T. Buttler, P. G. Kwiat, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. Glen Peterson, C. M. Simmons, "Secure communications using quantum cryptography," in *Proc. SPIE*, vol. 3076, pp. 2–11, 1997.
- [16] R. J. Hughes, G. L. Morgan, and C. Glen Peterson, "Quantum key distribution over a 48 km optical fibre network," *J. Mod. Opt.*, vol. 47, no. 2/3, pp. 533–547, 2000.

- [17] A. Poppe, A. Fedrizzi, T. Loruenser, O. Maurhardt, R. Ursin, H. R. Boehm, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, A. Zeilinger, "Practical quantum key distribution with polarization-entangled photons," Preprint: quant-ph/0404115, Available: <http://arxiv.org/abs/quant-ph/0404115>, 2004.
- [18] idQuantique SA (Geneve, Switzerland), <http://www.idquantique.com>
- [19] Magiq technologies (Sommerville, USA), <http://www.magiqtech.com>
- [20] NEC Ltd. (Tokyo, Japan), <http://www.nec.com>
- [21] F. Tamburini, C. Barbieri, S. Ortolani, and A. Bianchini, "Futuristic applications of quantum EPR states," in *Proc. Italian Astronomical Society*, vol. 74, no. 2, 2002.
- [22] F. Tamburini and C. Barbieri, "Futuristic applications of quantum information and communication," in *Proc. Futuristic Space Technologies*, ASI workshop, 2002.
- [23] D. Bouwmeester, A. Ekert, and A. Zeilinger (eds.), *The Physics of Quantum Information*, Springer, 2000.