Shannon's Legacy: Coding Theory from 1948-2016

Daniel J. Costello, Jr.

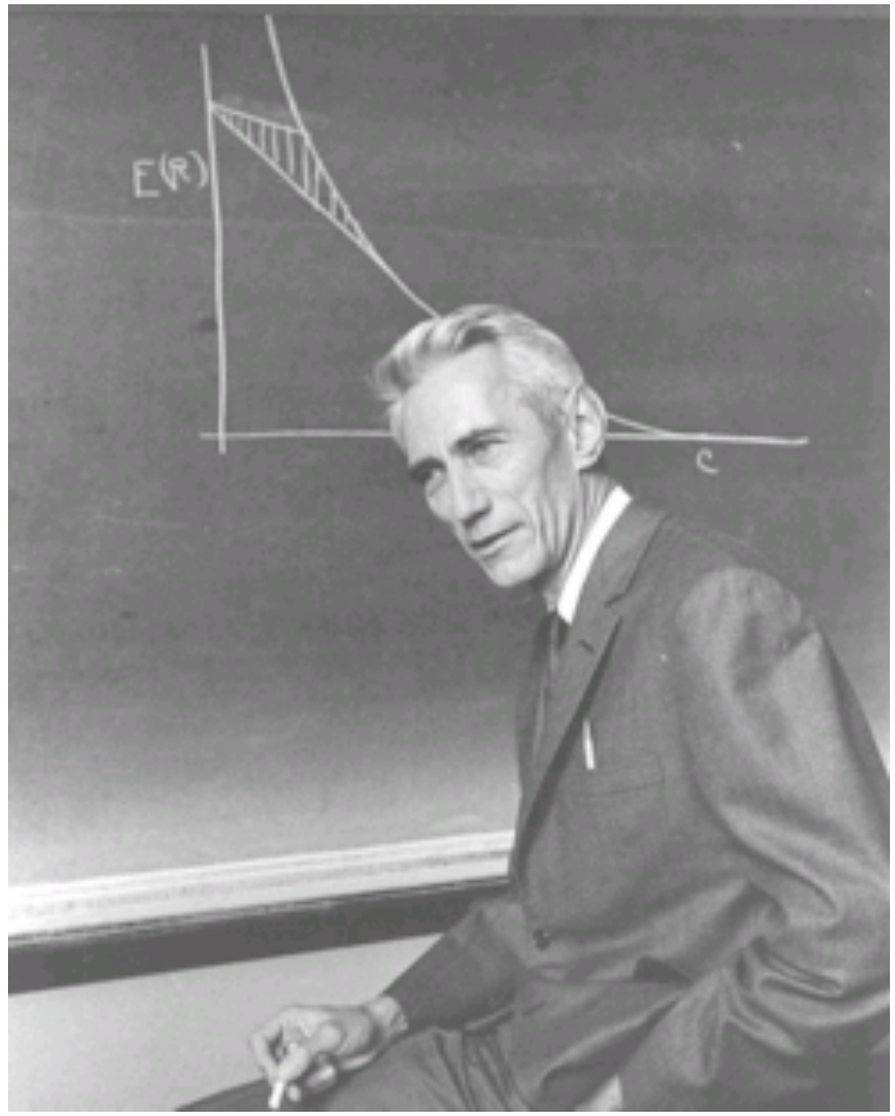
Coding Research Group
Department of Electrical Engineering
University of Notre Dame
Notre Dame, IN 46556

Shannon Day
Kanpur, India
October 19, 2016

The author gratefully acknowledges the help of Lance C. Perez, Hermano A. Cabral, Oscar Y. Takeshita, Adrish Banerjee, Ali Pusane, and David Mitchell in the preparation of this presentation.

In the Beginning...

In the Beginning...



Claude Elwood Shannon
Apr 30, 1916 – Feb 24, 2001
Father of Information Theory

In the Beginning...

Shannon's Theory Was Invented at Bell Labs

Bell Labs in Murray Hill,
New Jersey

In the Beginning...

In the Beginning...

Three Great Successes of Information Theory

In the Beginning...

Three Great Successes of Information Theory

- Source Coding for Data Compression

In the Beginning...

Three Great Successes of Information Theory

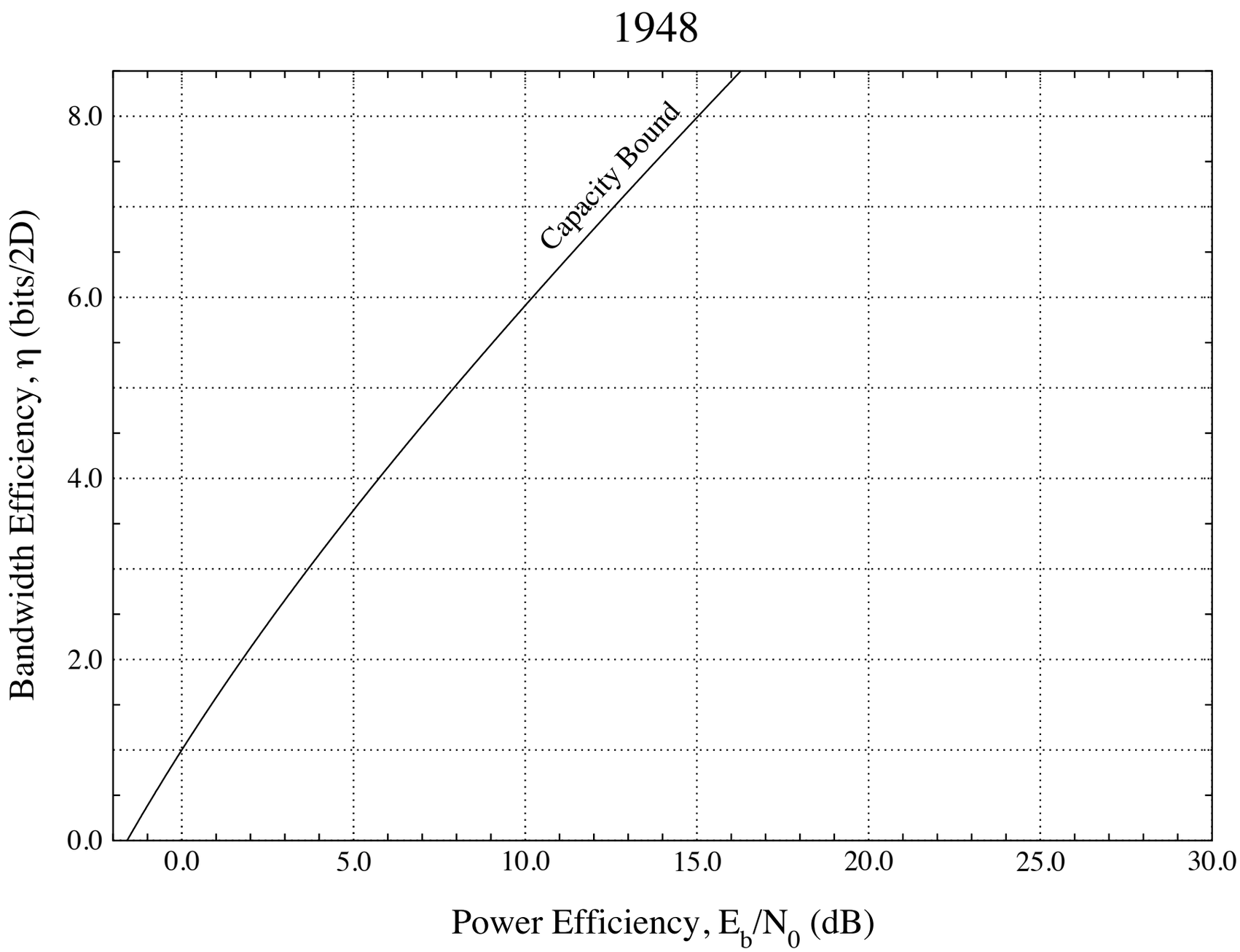
- Source Coding for Data Compression
- Secret Coding (Cryptography) for Data Security

In the Beginning...

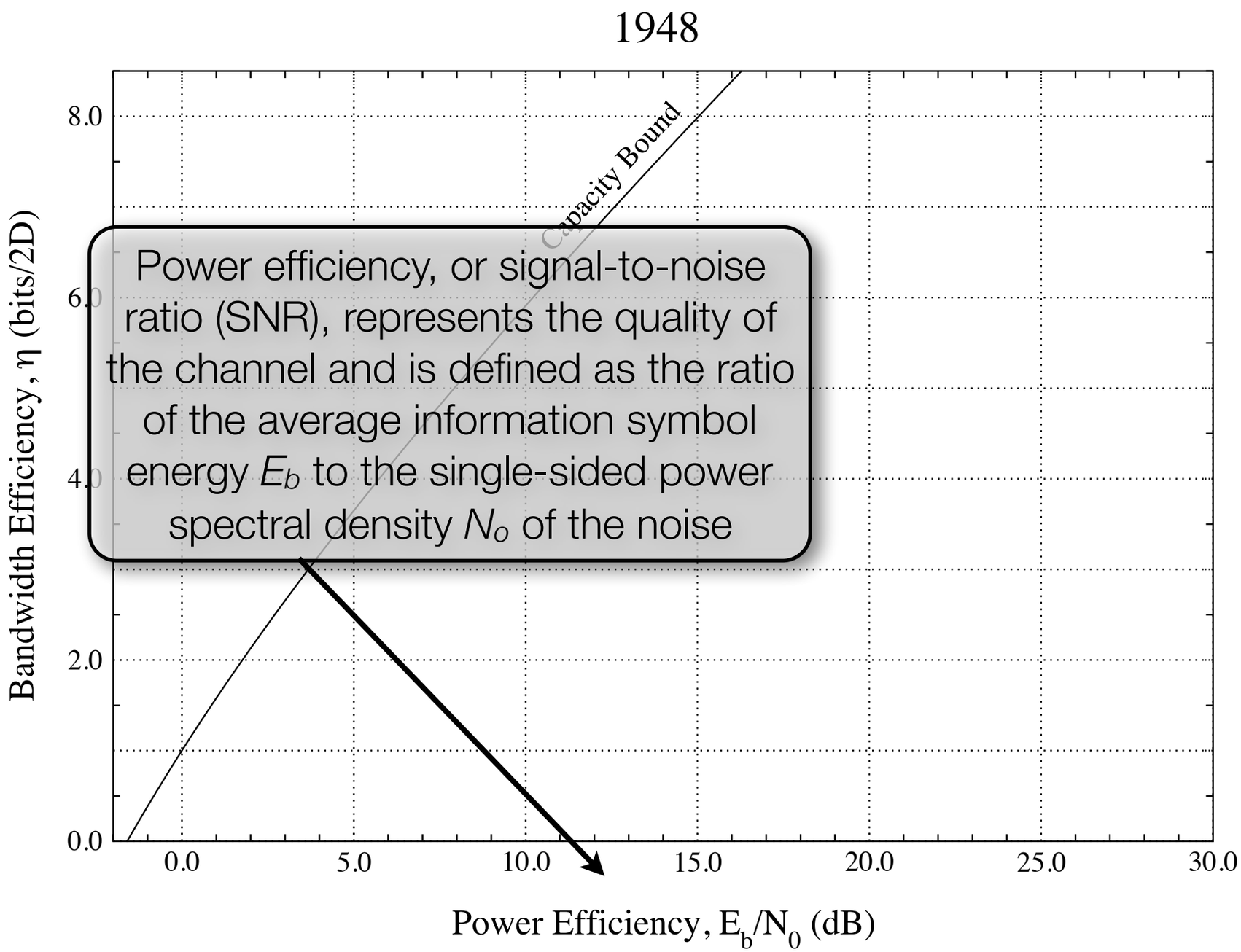
Three Great Successes of Information Theory

- Source Coding for Data Compression
- Secret Coding (Cryptography) for Data Security
- Channel Coding for Data Reliability (*the focus of this presentation*)

In the Beginning

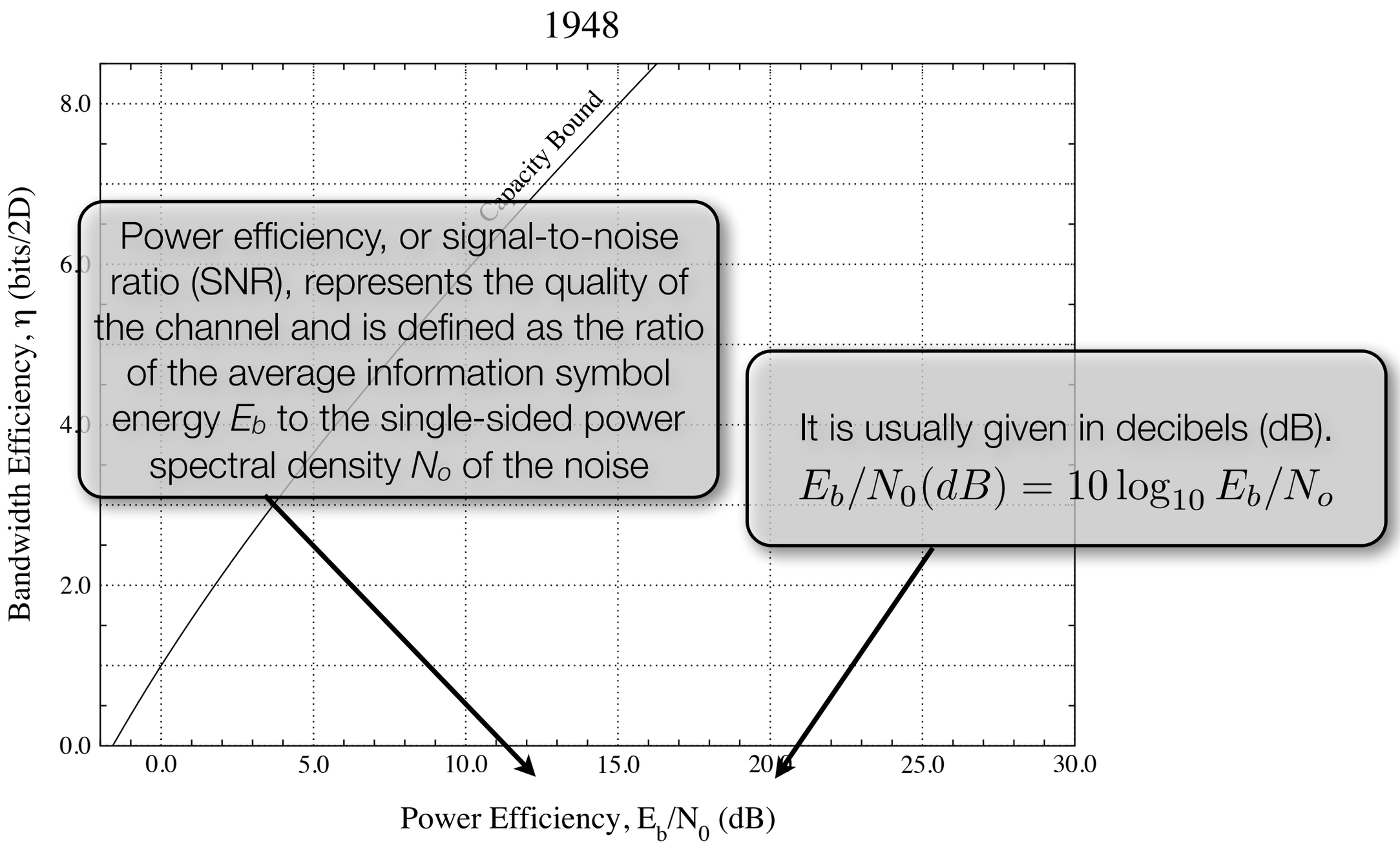


In the Beginning

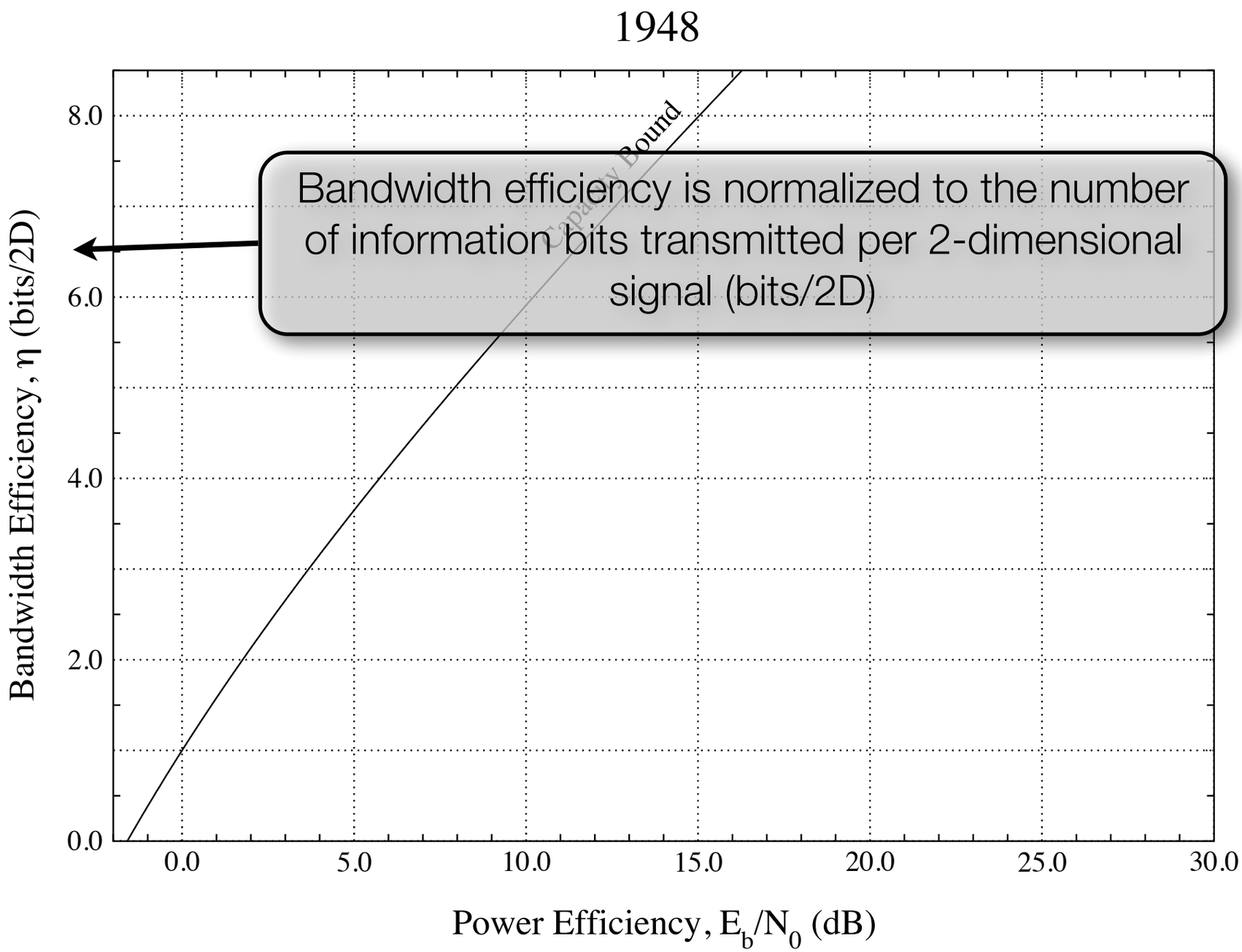


Power efficiency, or signal-to-noise ratio (SNR), represents the quality of the channel and is defined as the ratio of the average information symbol energy E_b to the single-sided power spectral density N_o of the noise

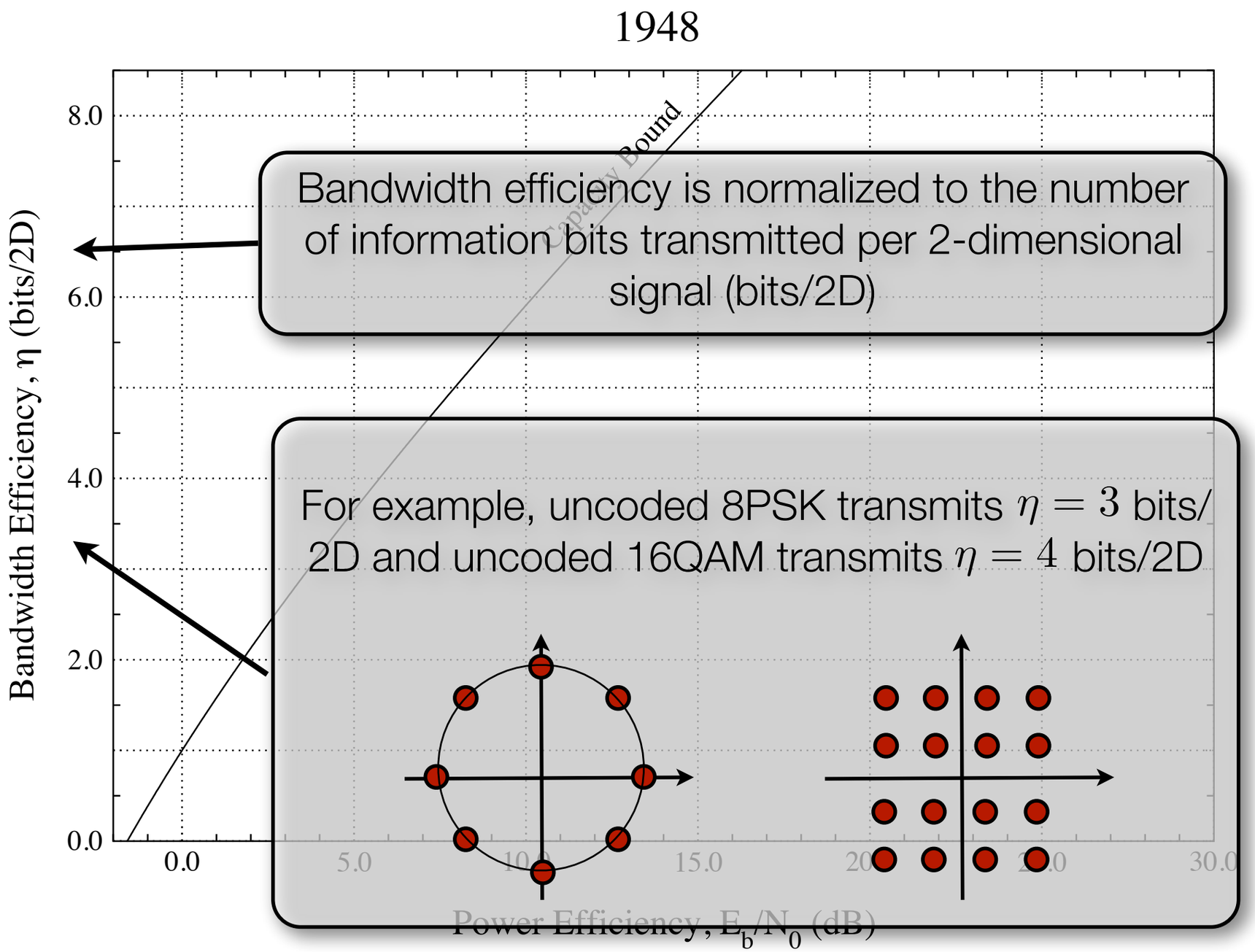
In the Beginning



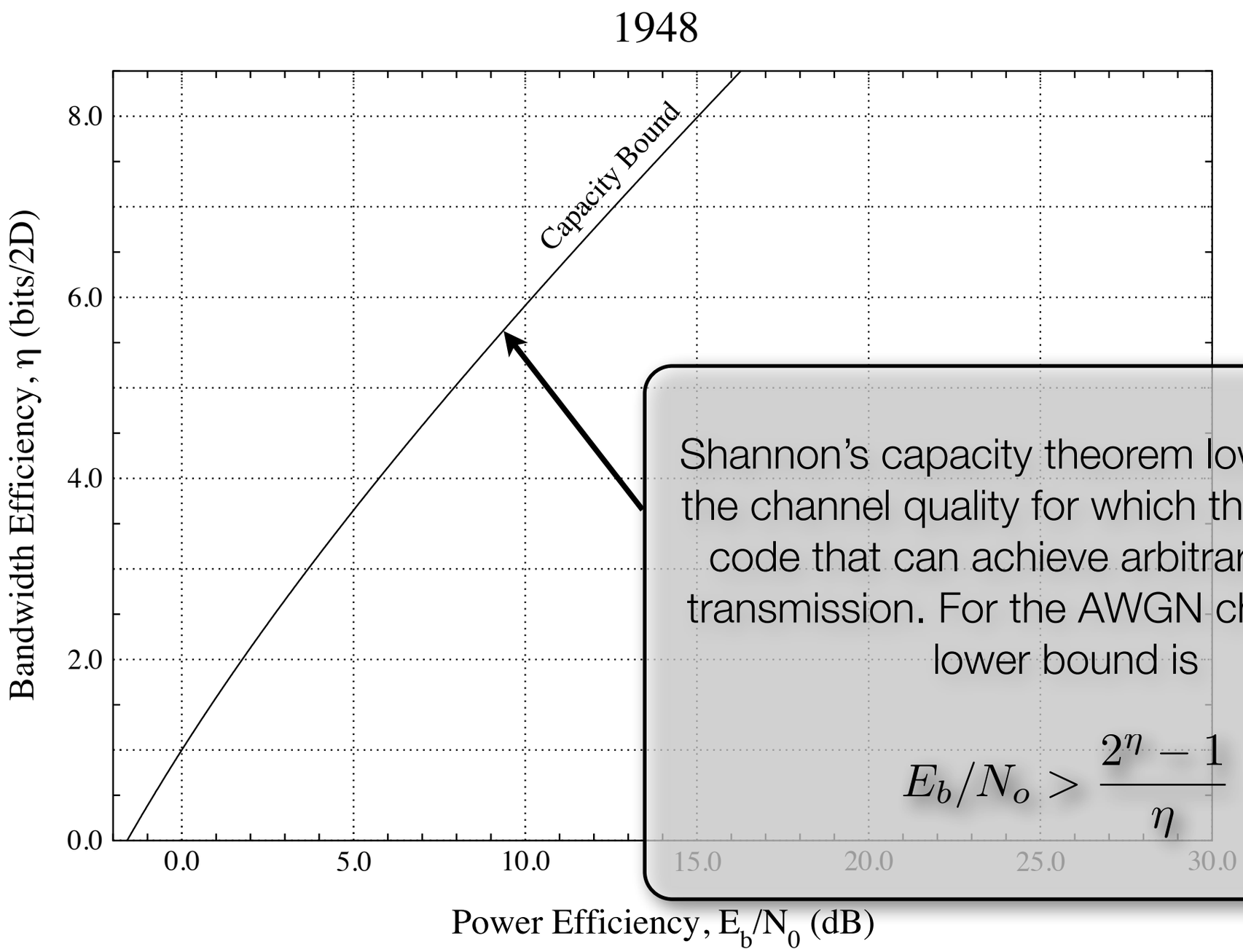
In the Beginning



In the Beginning



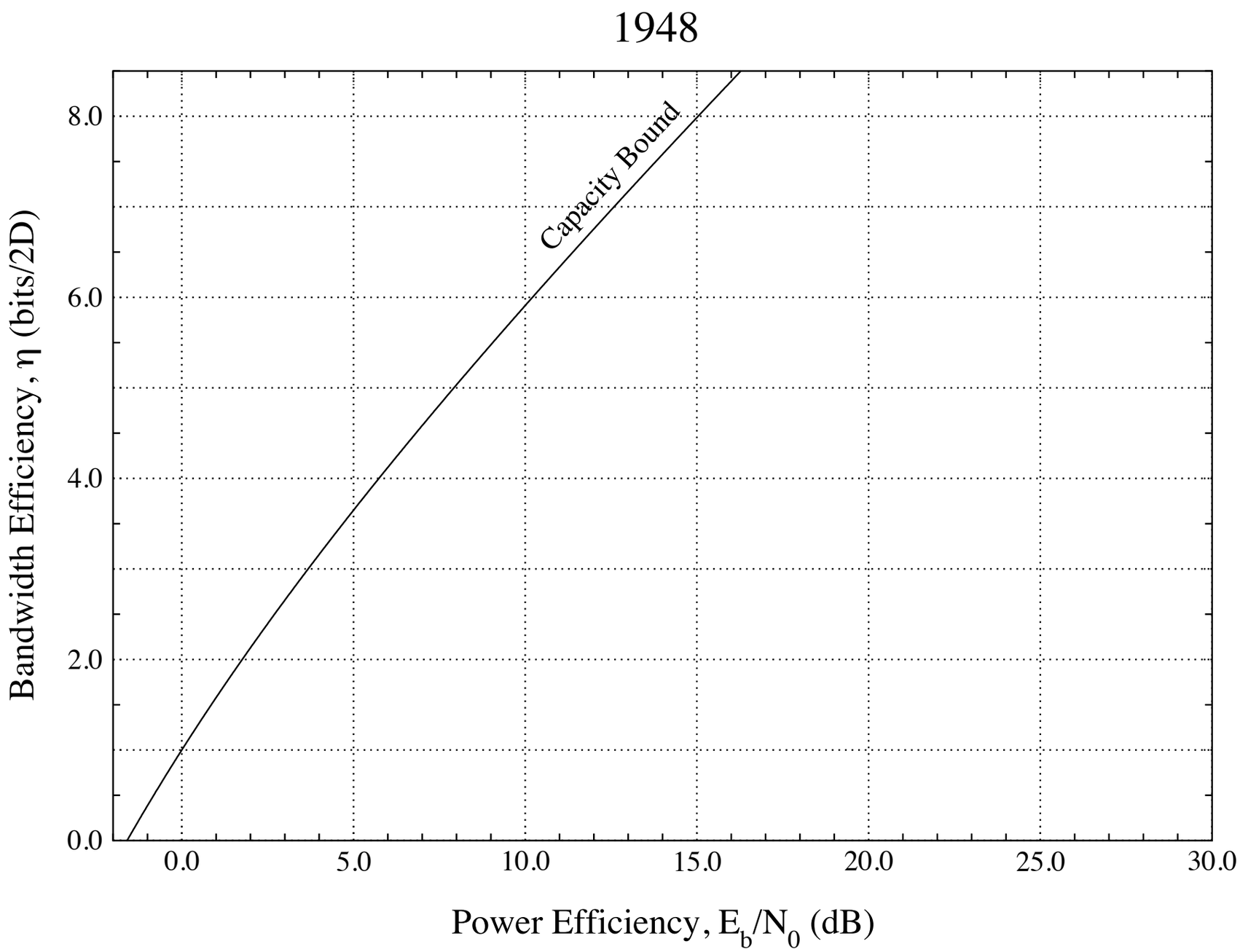
In the Beginning



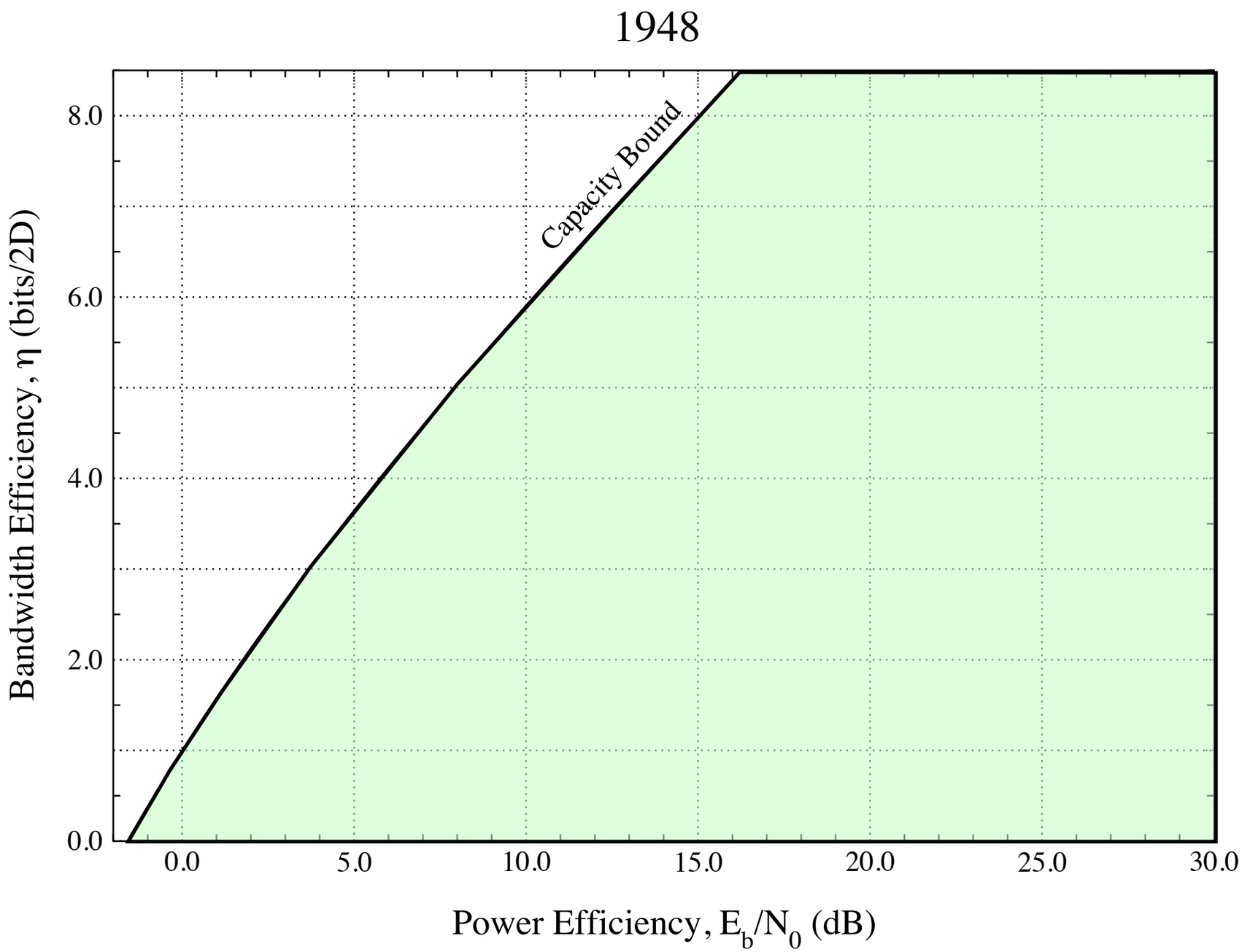
Shannon's capacity theorem lower bounds the channel quality for which there exists a code that can achieve arbitrarily reliable transmission. For the AWGN channel, this lower bound is

$$E_b/N_o > \frac{2^\eta - 1}{\eta}$$

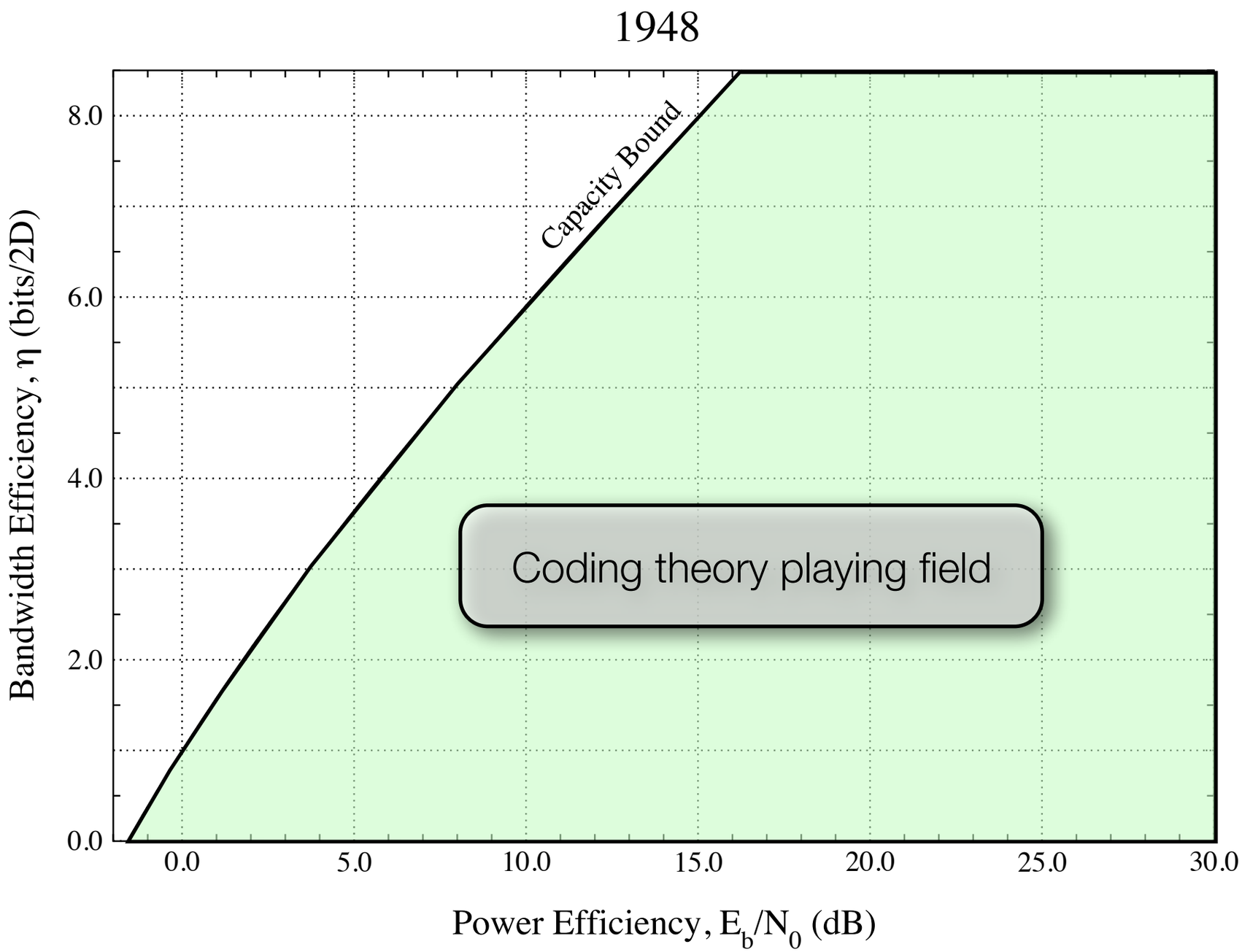
In the Beginning



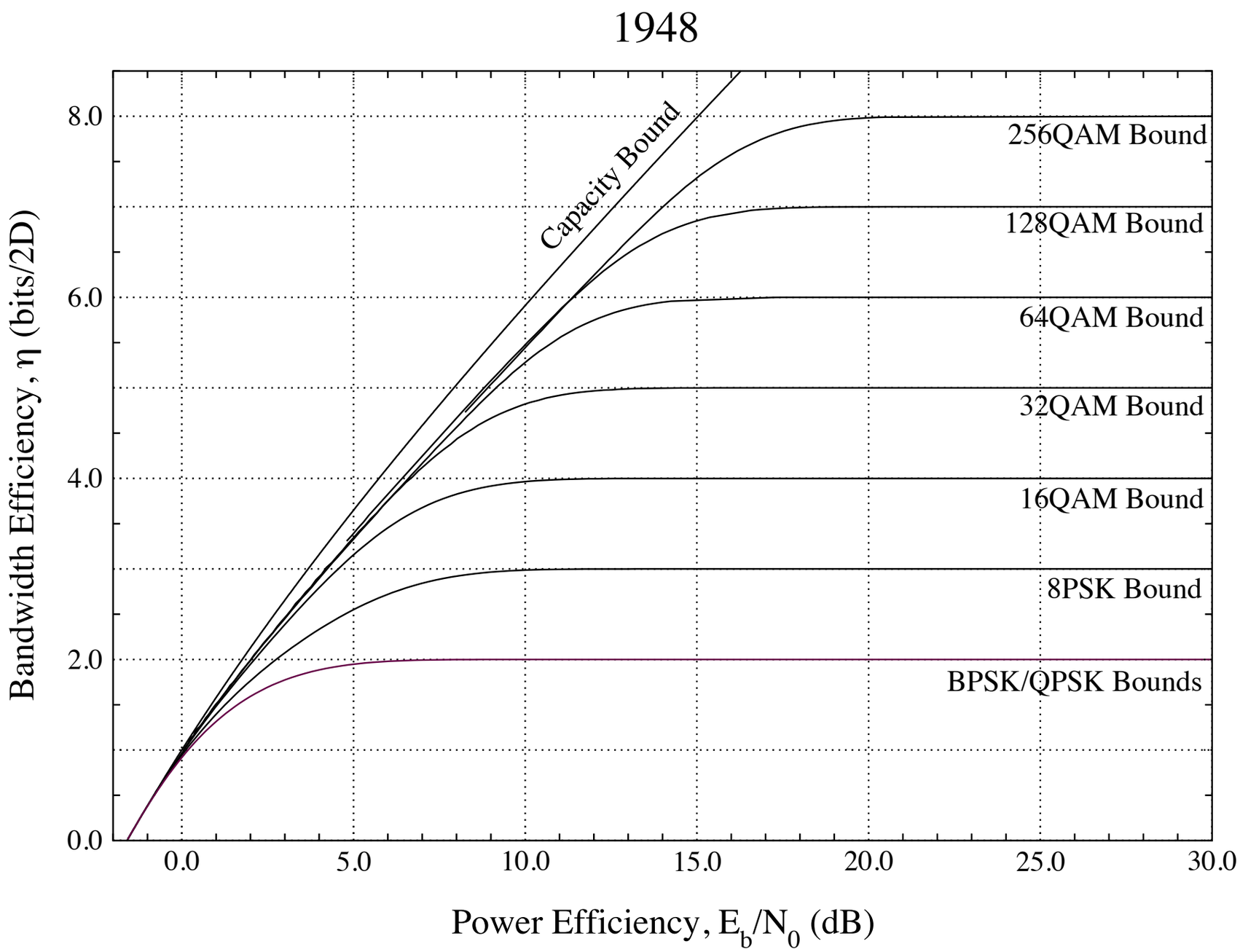
In the Beginning



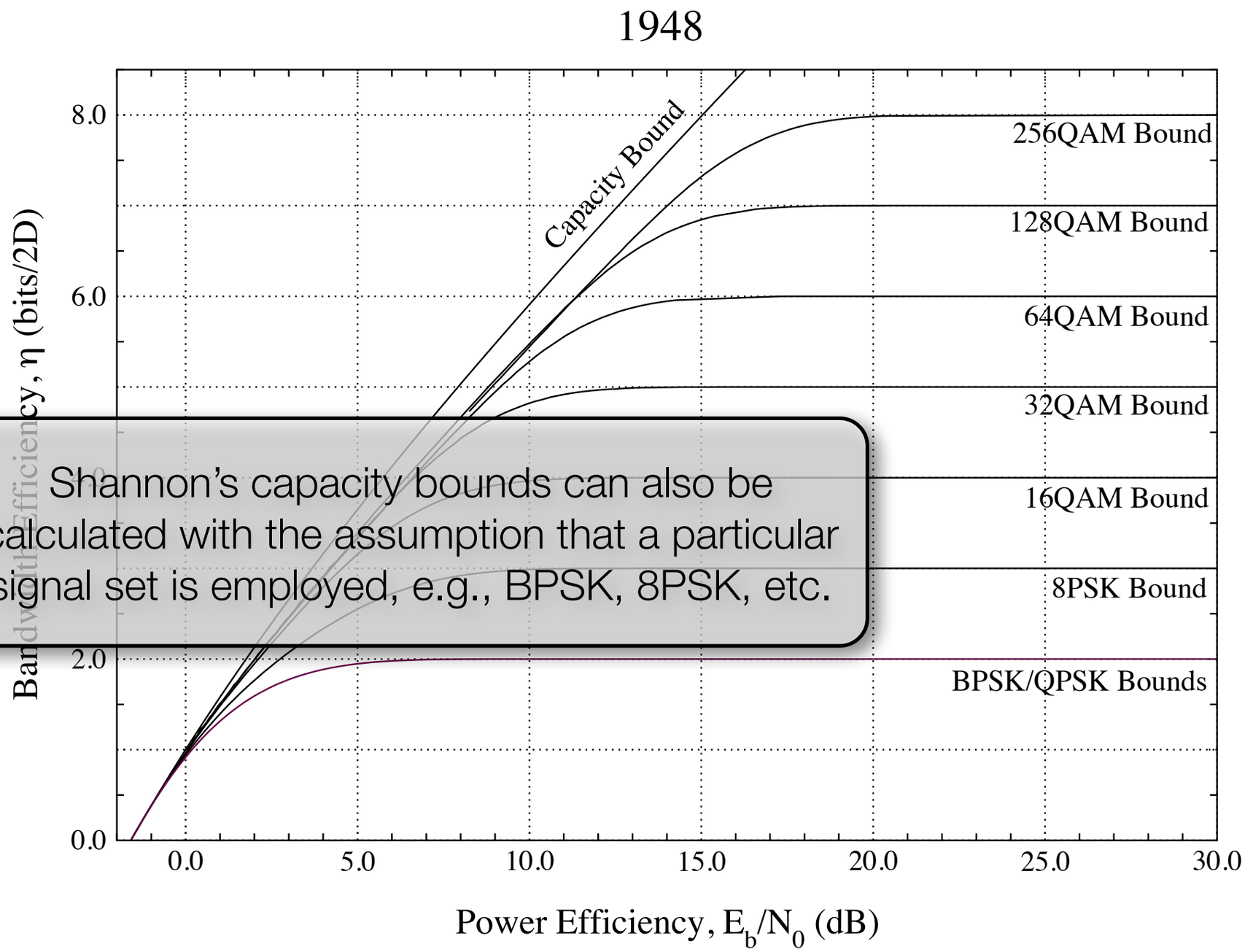
In the Beginning



In the Beginning

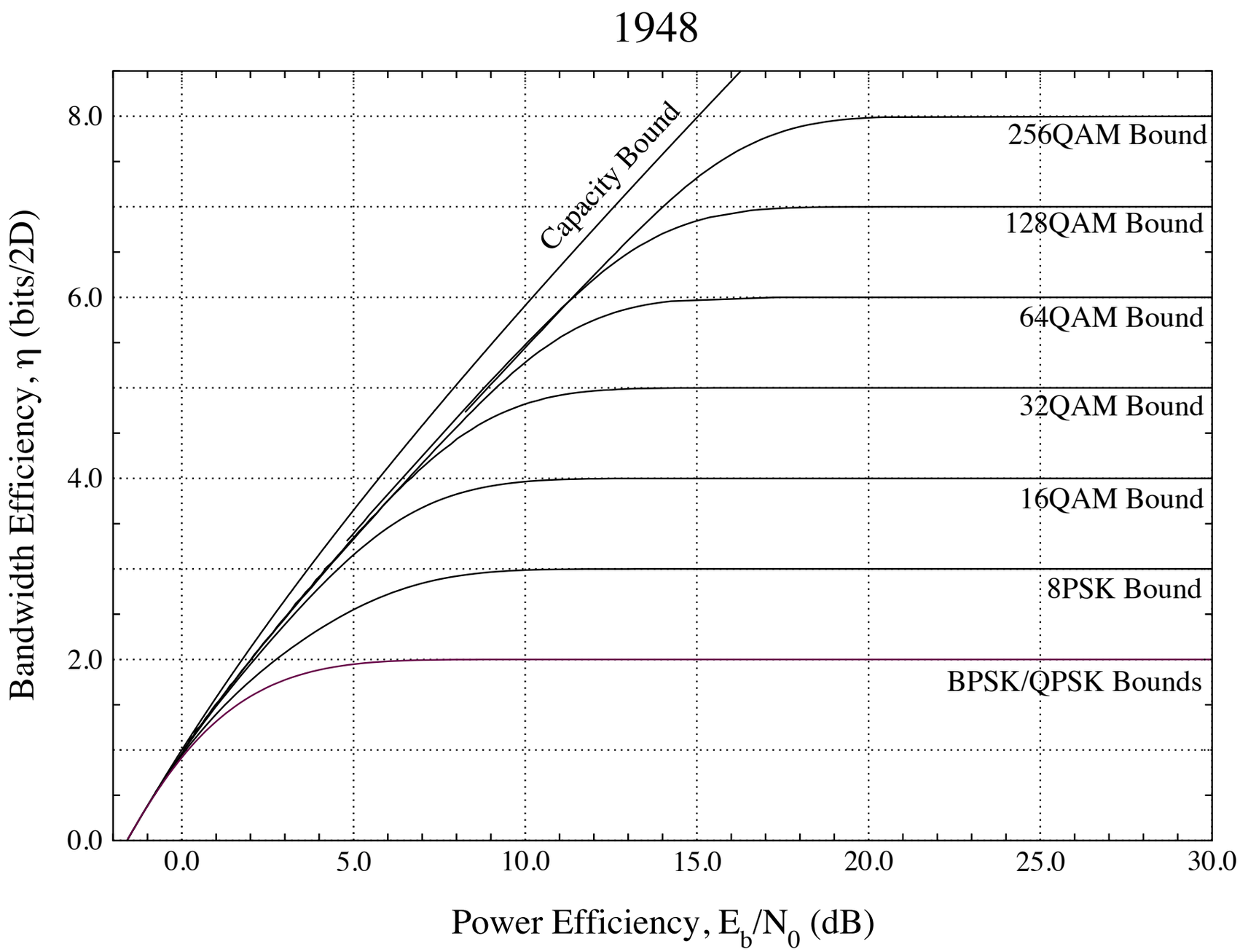


In the Beginning

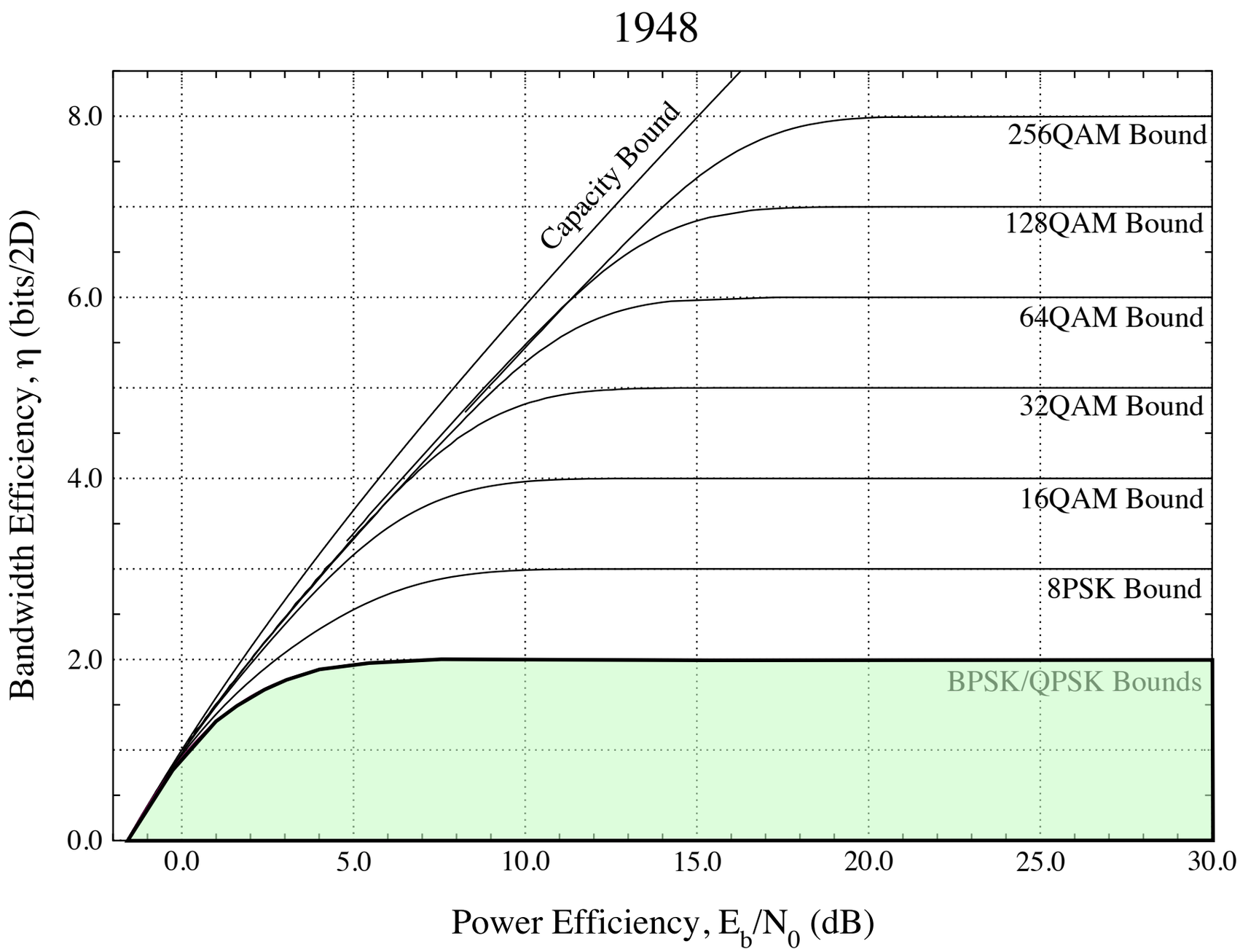


Shannon's capacity bounds can also be calculated with the assumption that a particular signal set is employed, e.g., BPSK, 8PSK, etc.

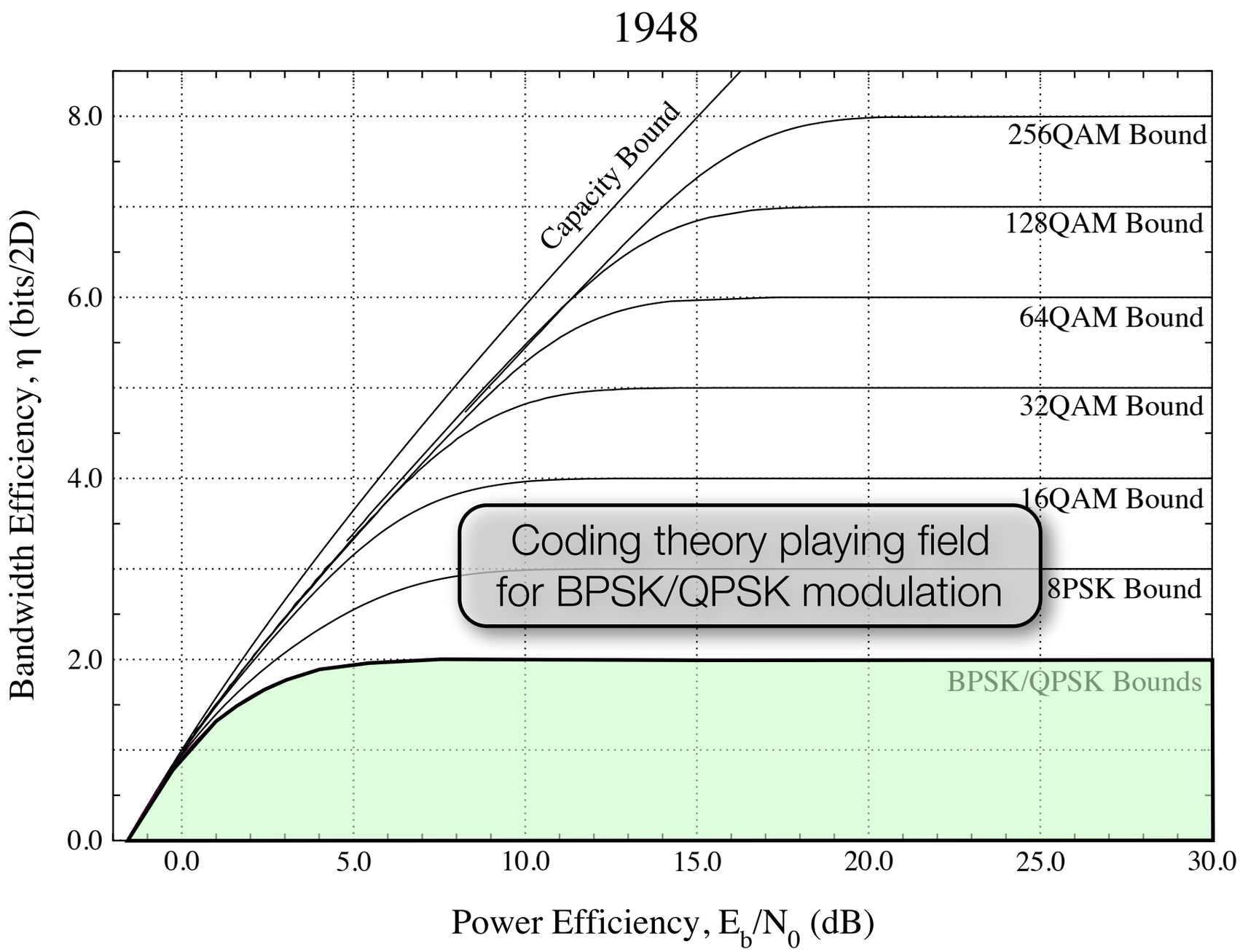
In the Beginning



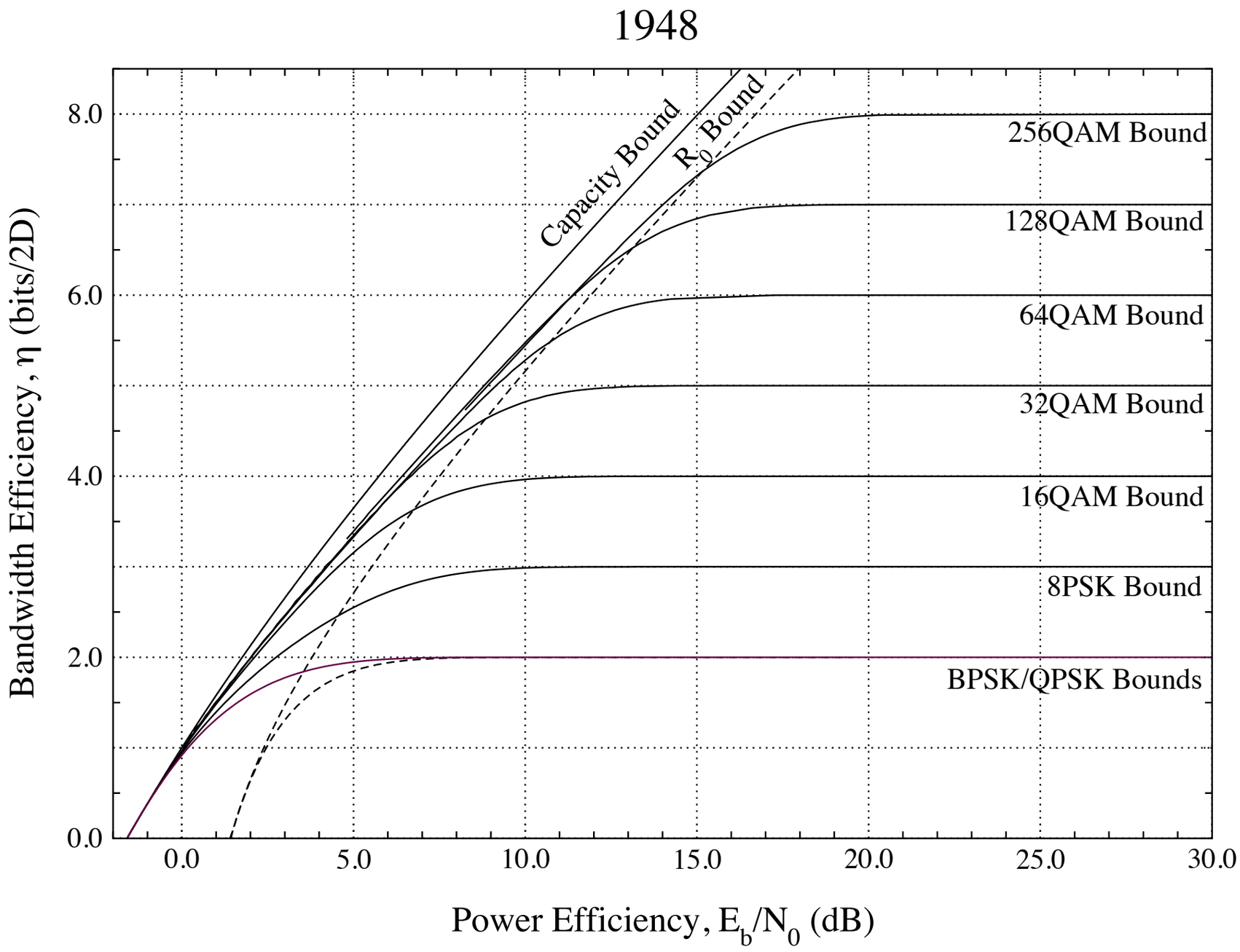
In the Beginning



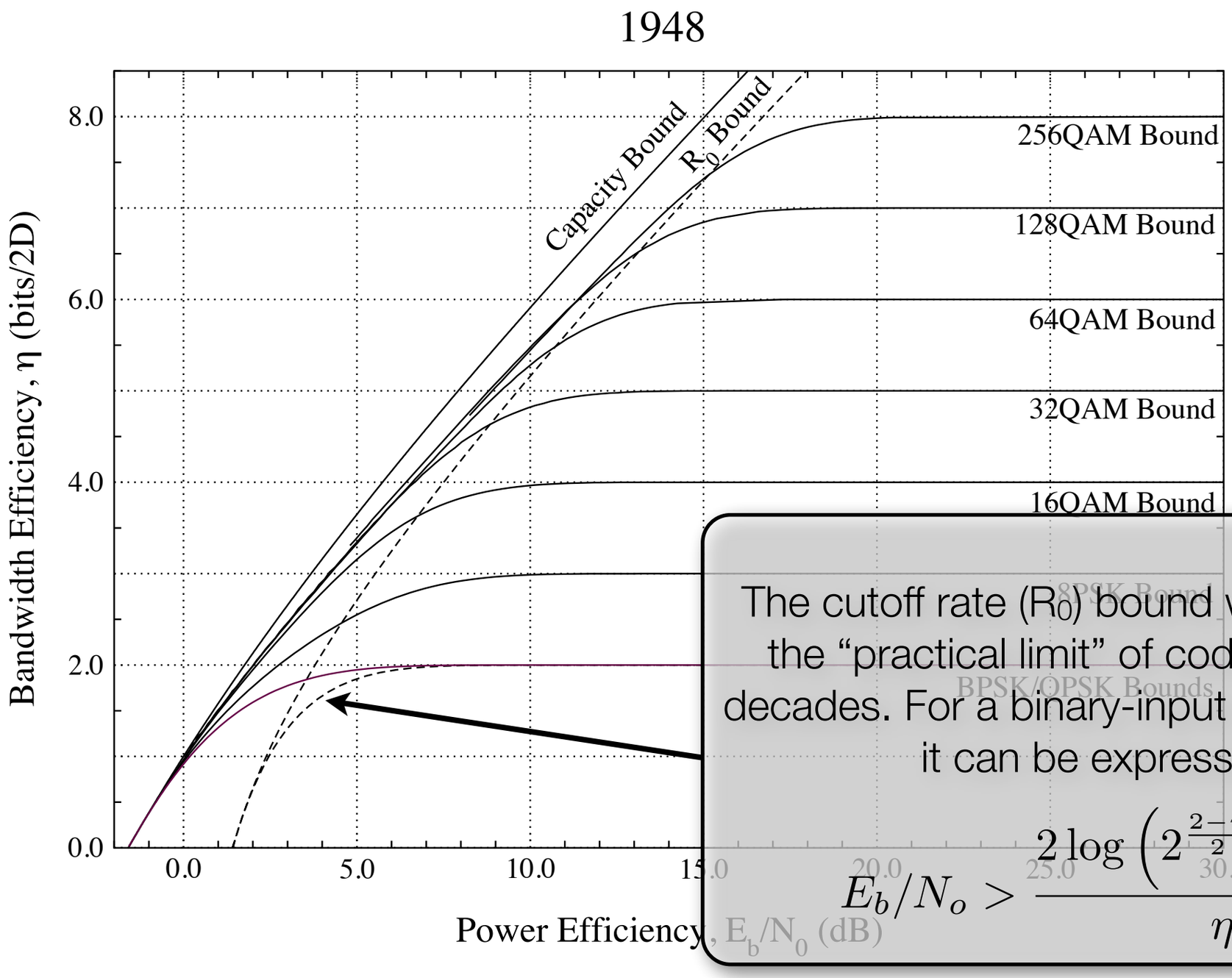
In the Beginning



In the Beginning



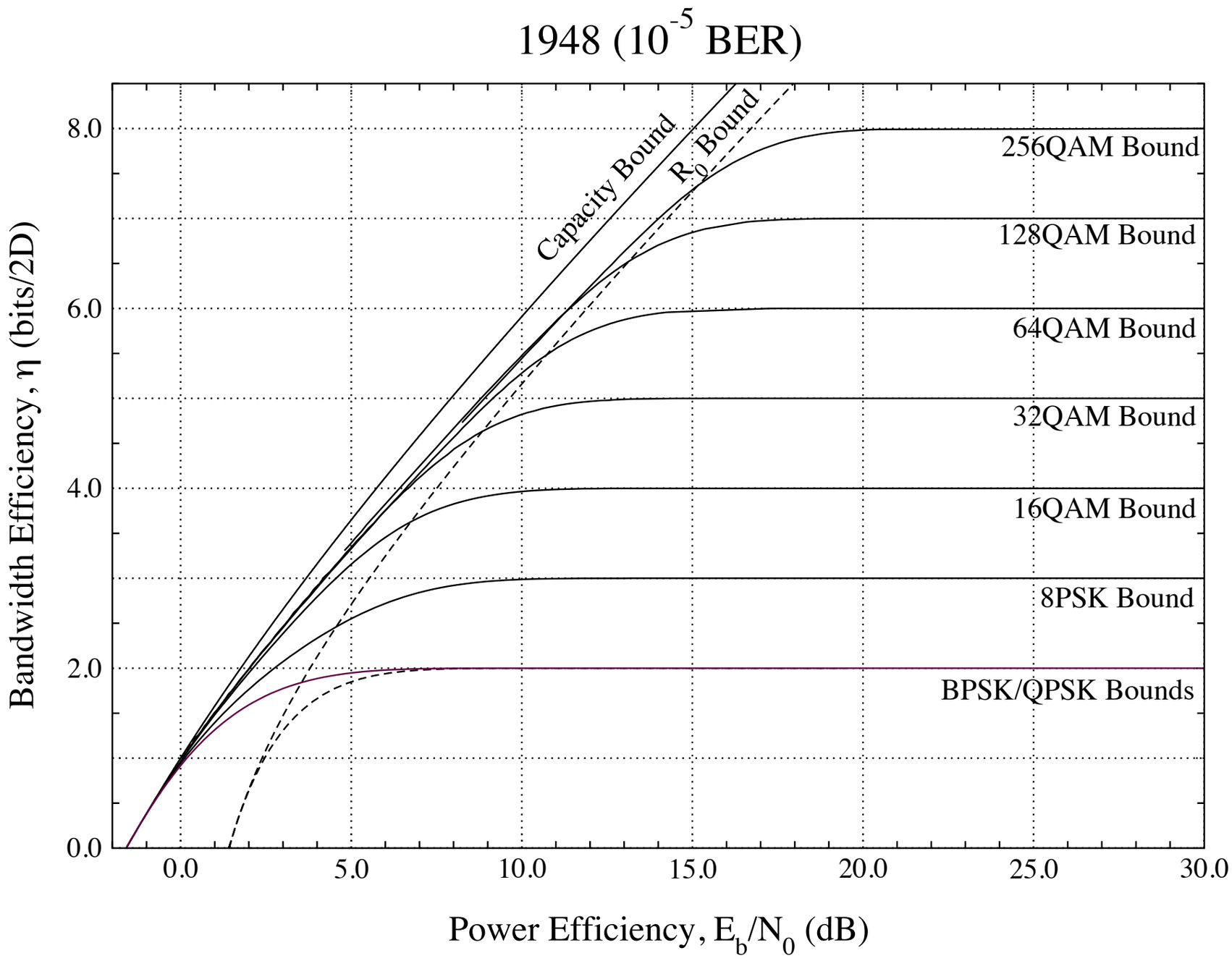
In the Beginning



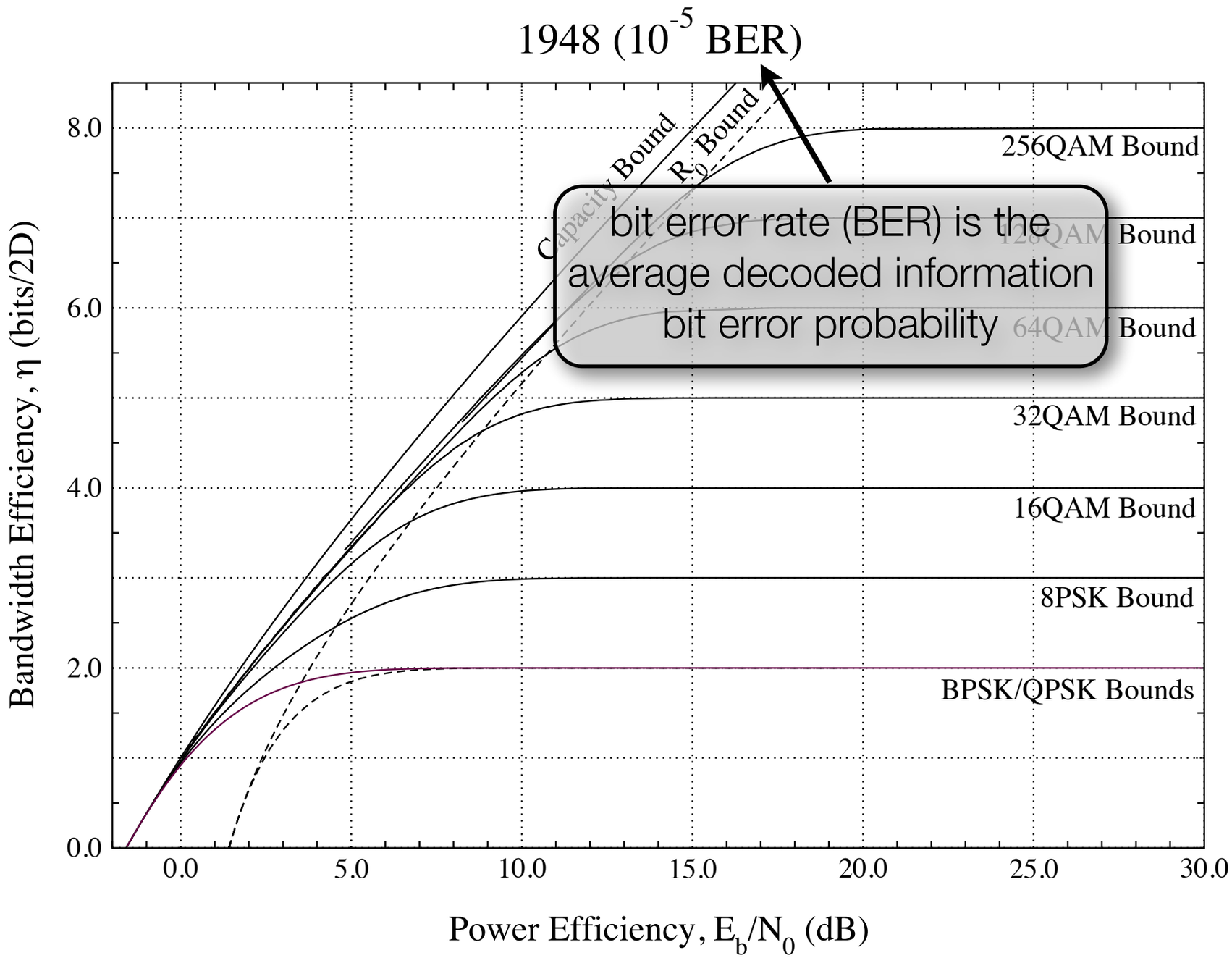
The cutoff rate (R_0) bound was considered the "practical limit" of coding for several decades. For a binary-input AWGN channel, it can be expressed as

$$E_b/N_o > \frac{2\log\left(2^{\frac{2-\eta}{2}}-1\right)^{-1}}{\eta}$$

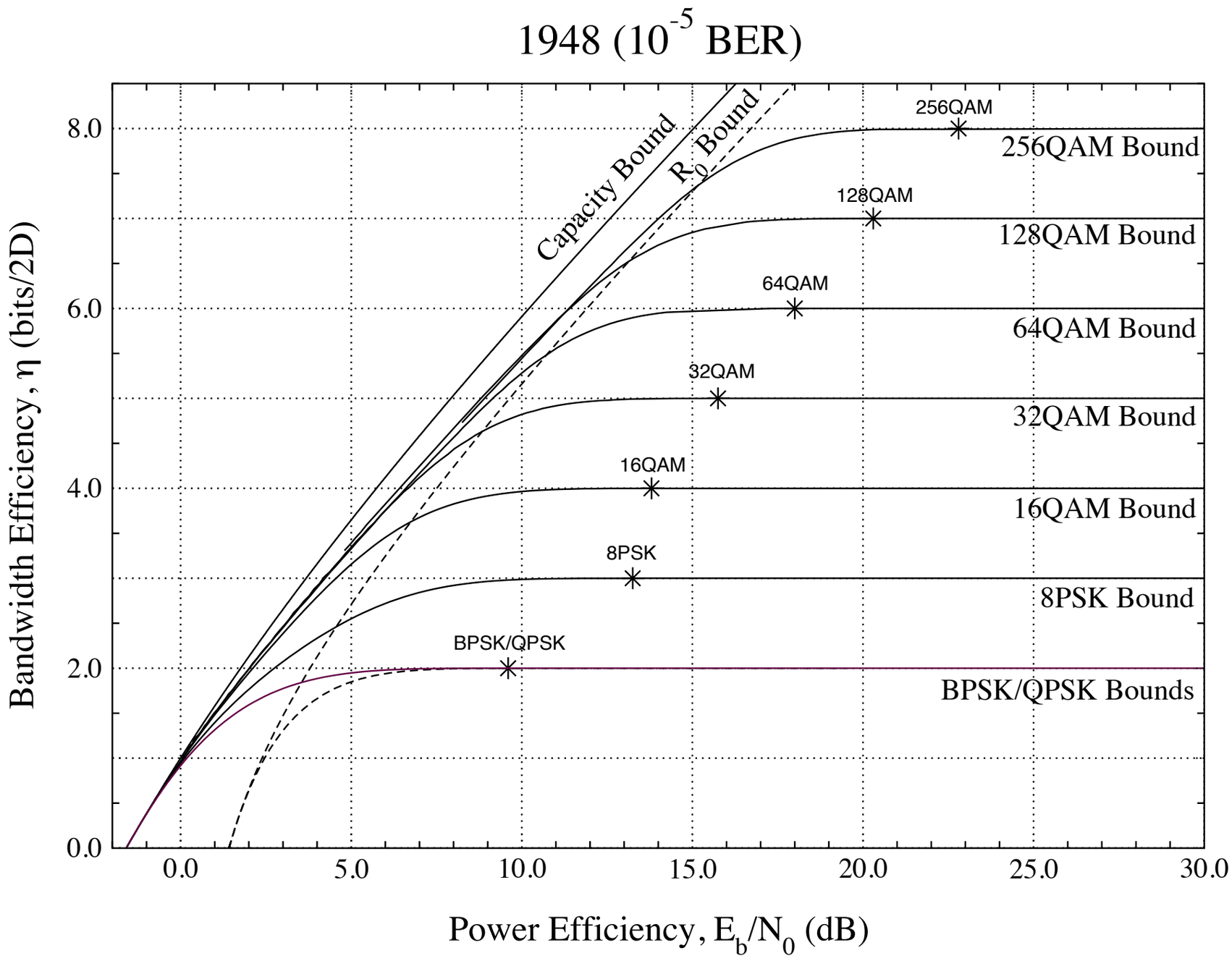
In the Beginning



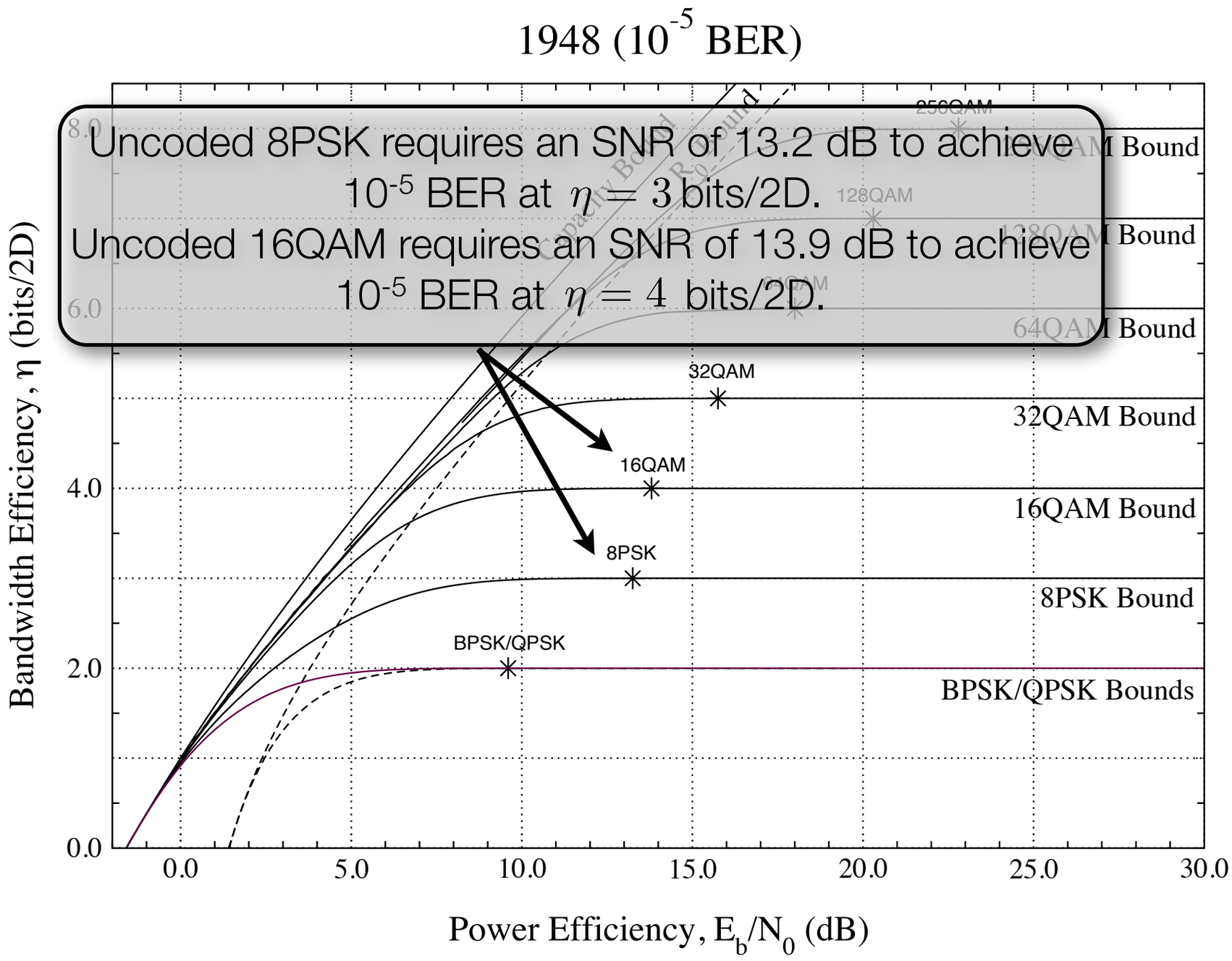
In the Beginning



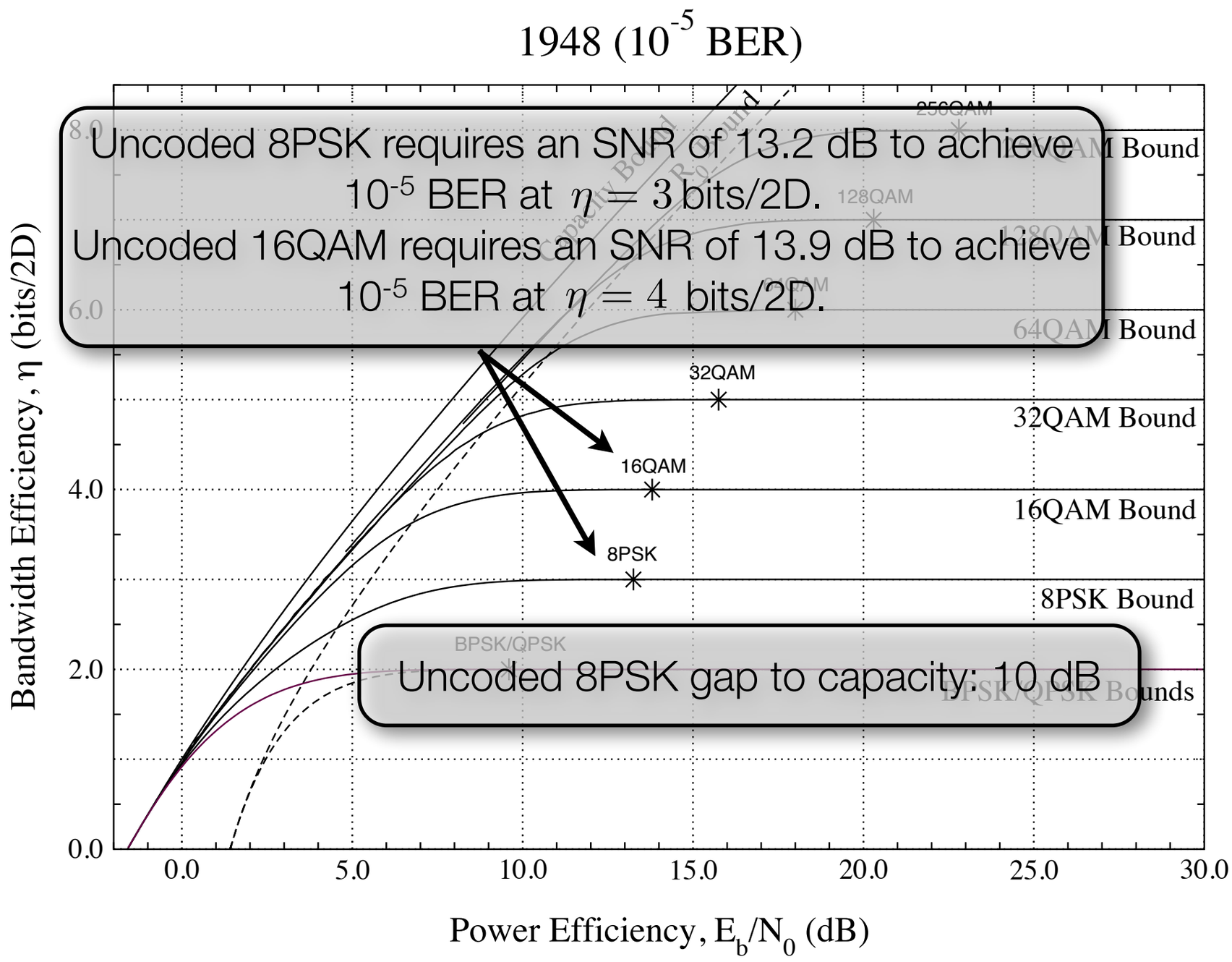
In the Beginning



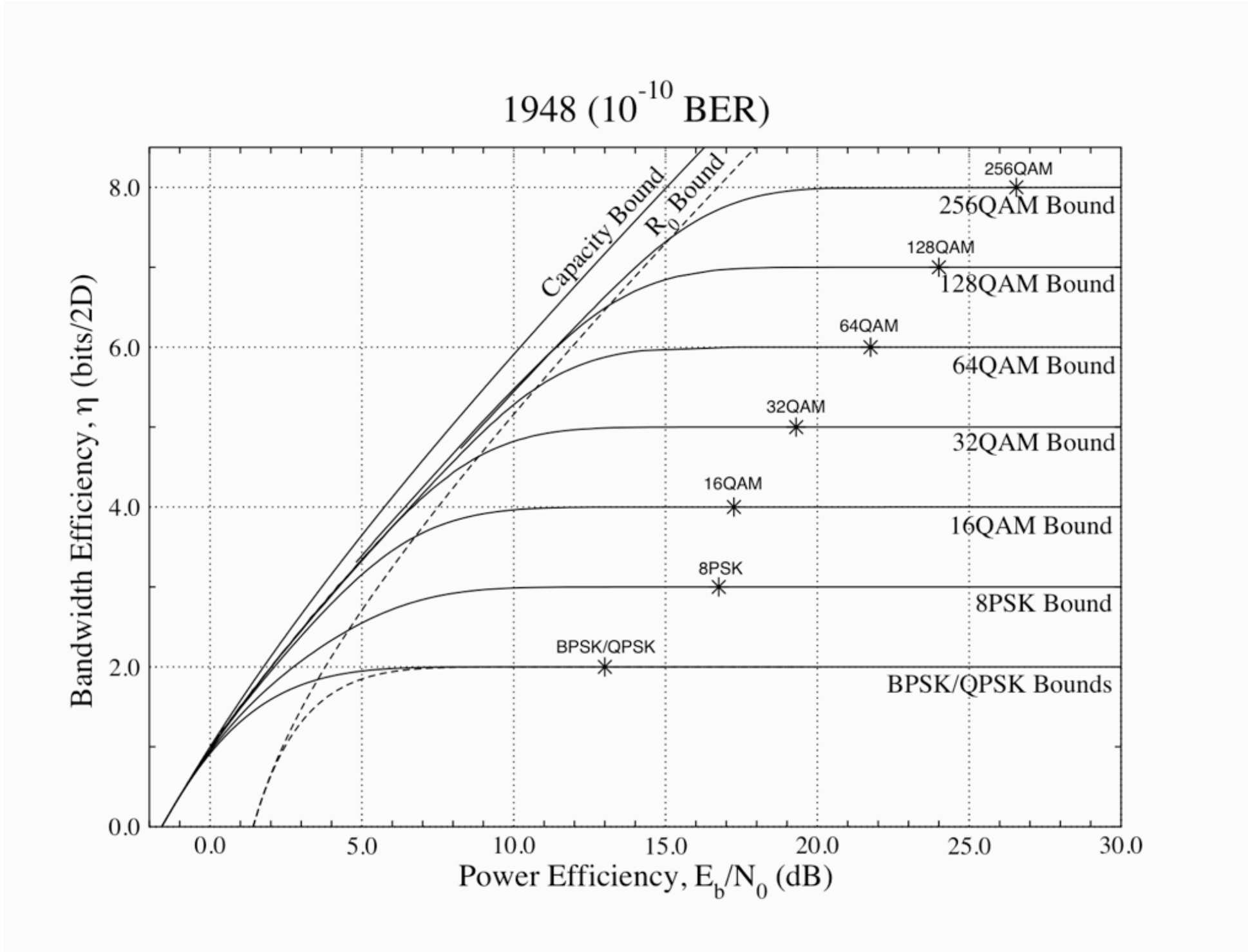
In the Beginning



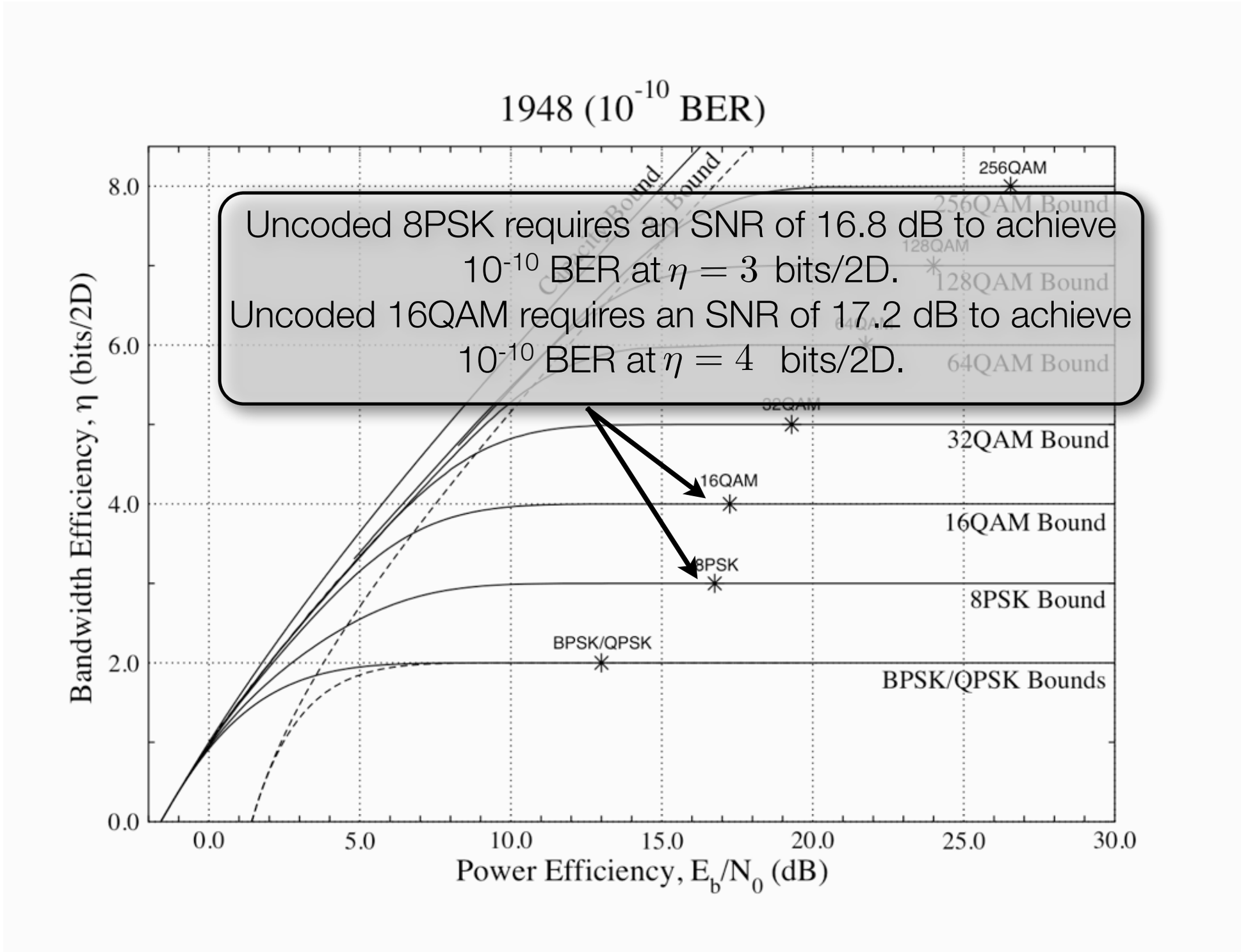
In the Beginning



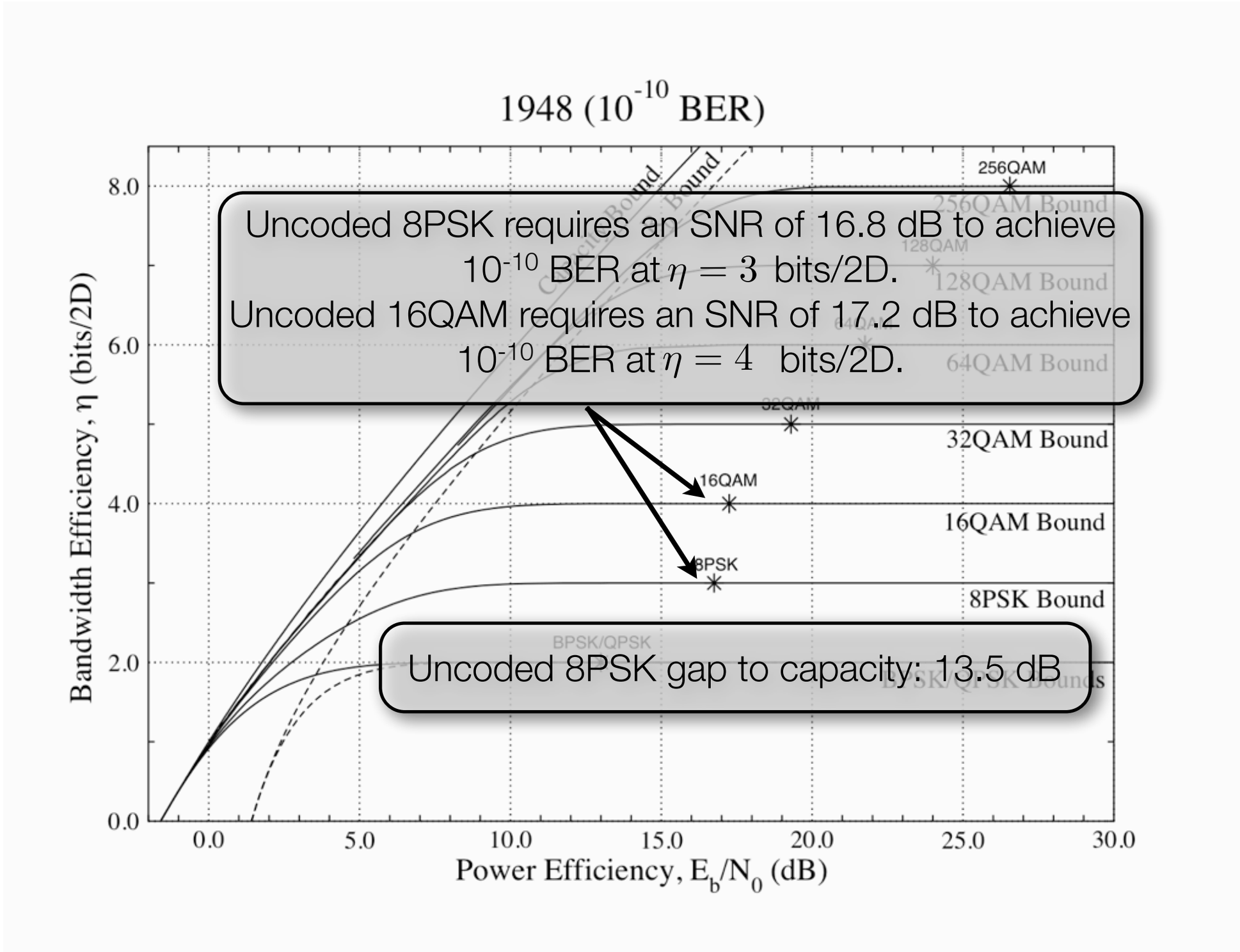
In the Beginning



In the Beginning

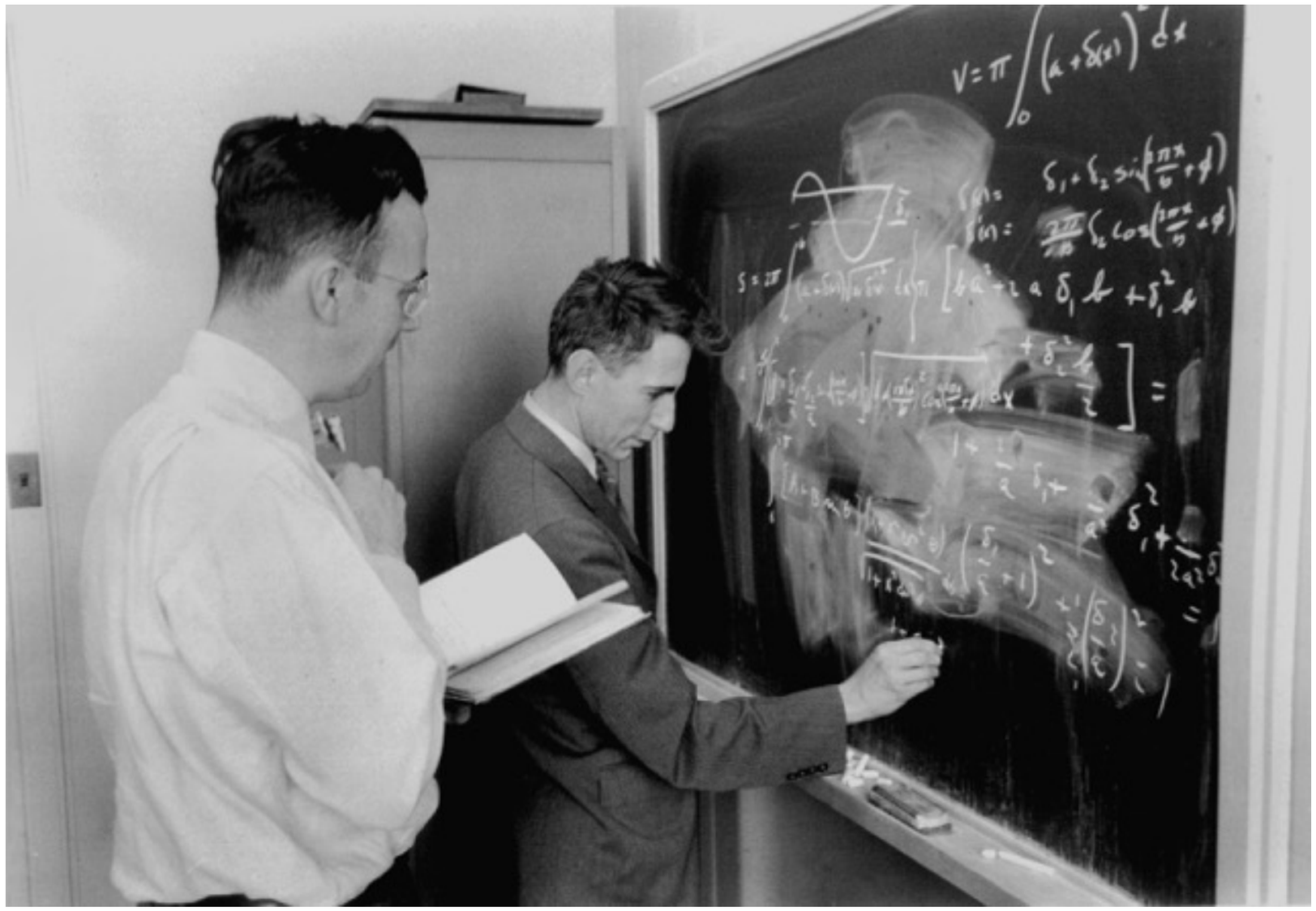


In the Beginning

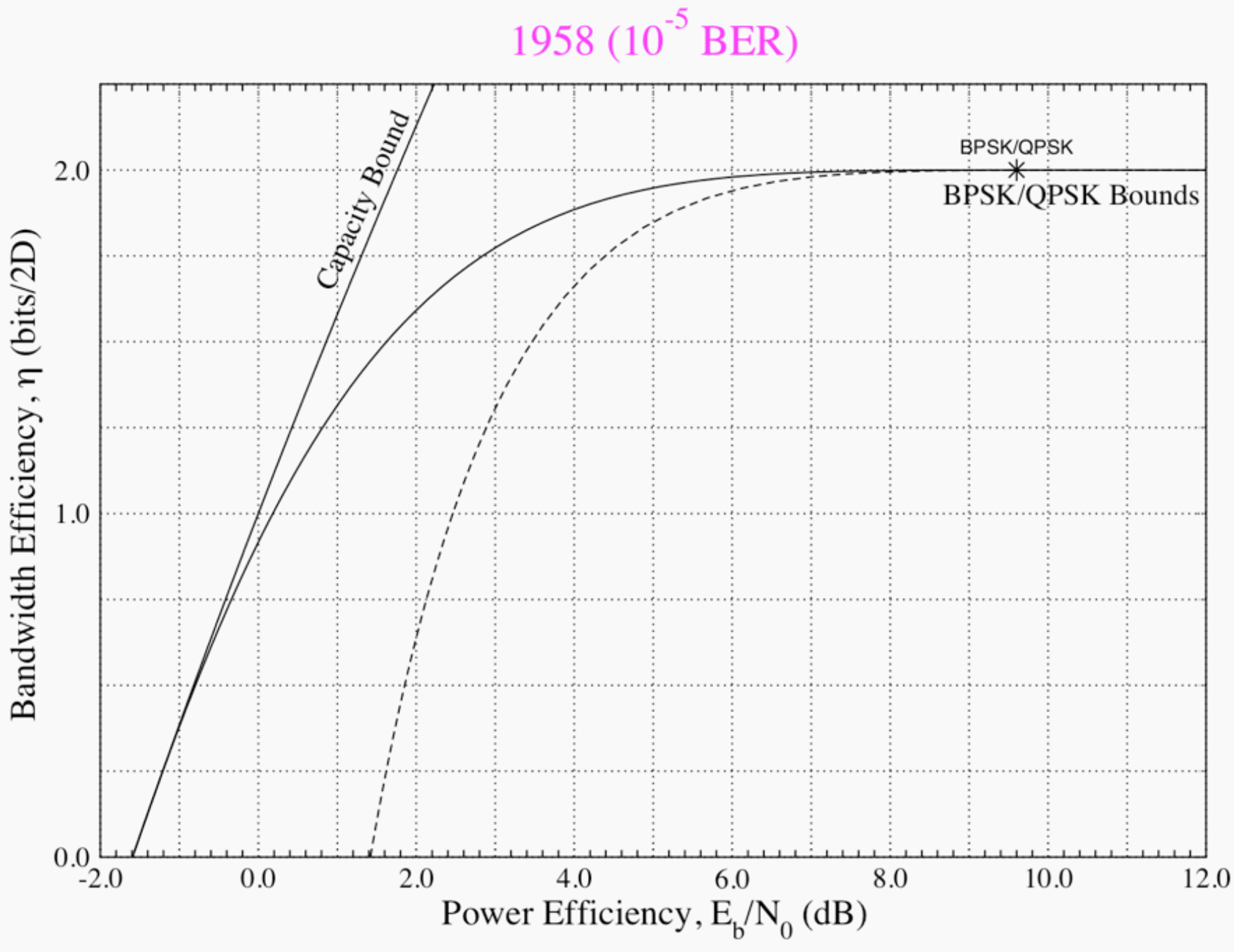


The First Day

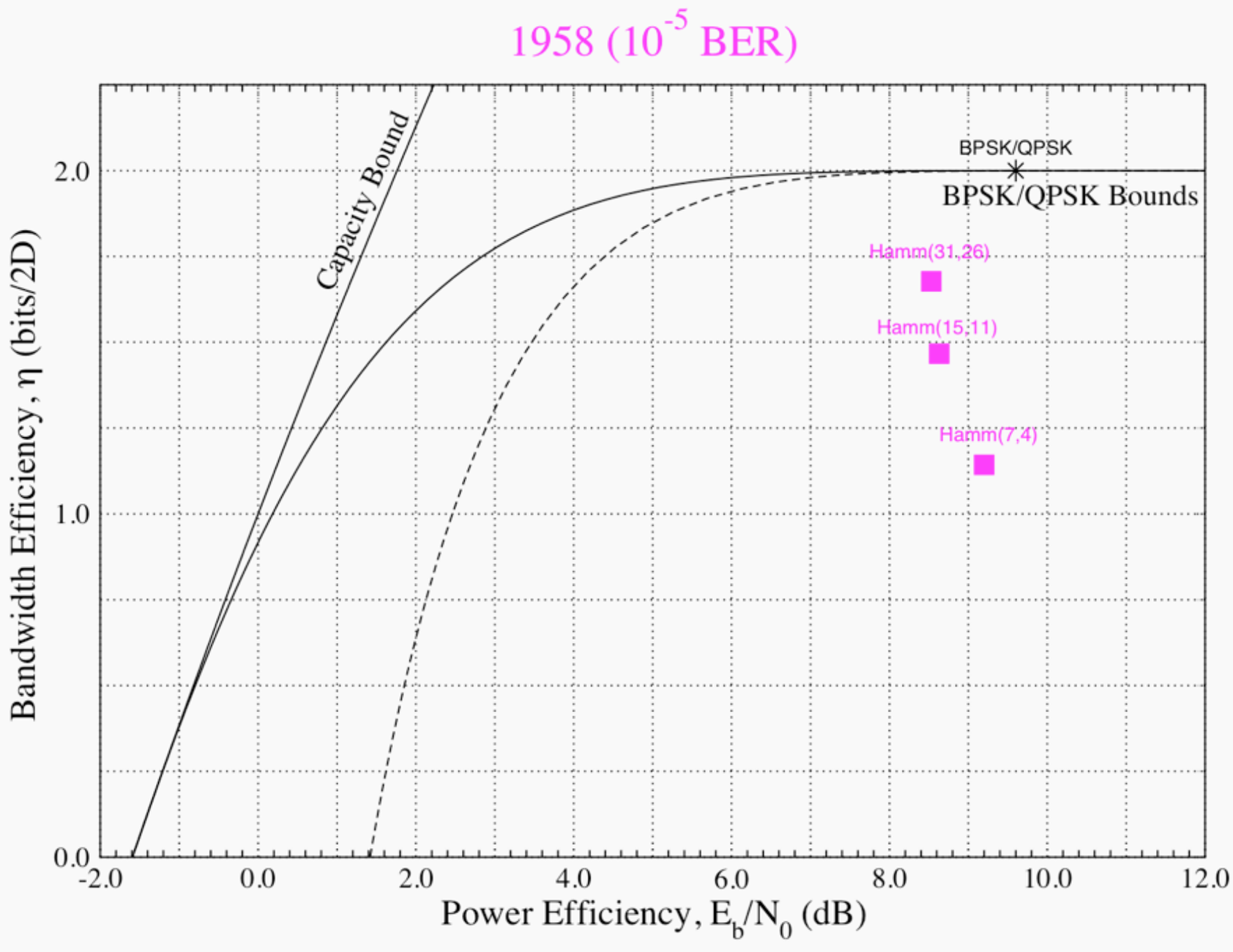
The First Day



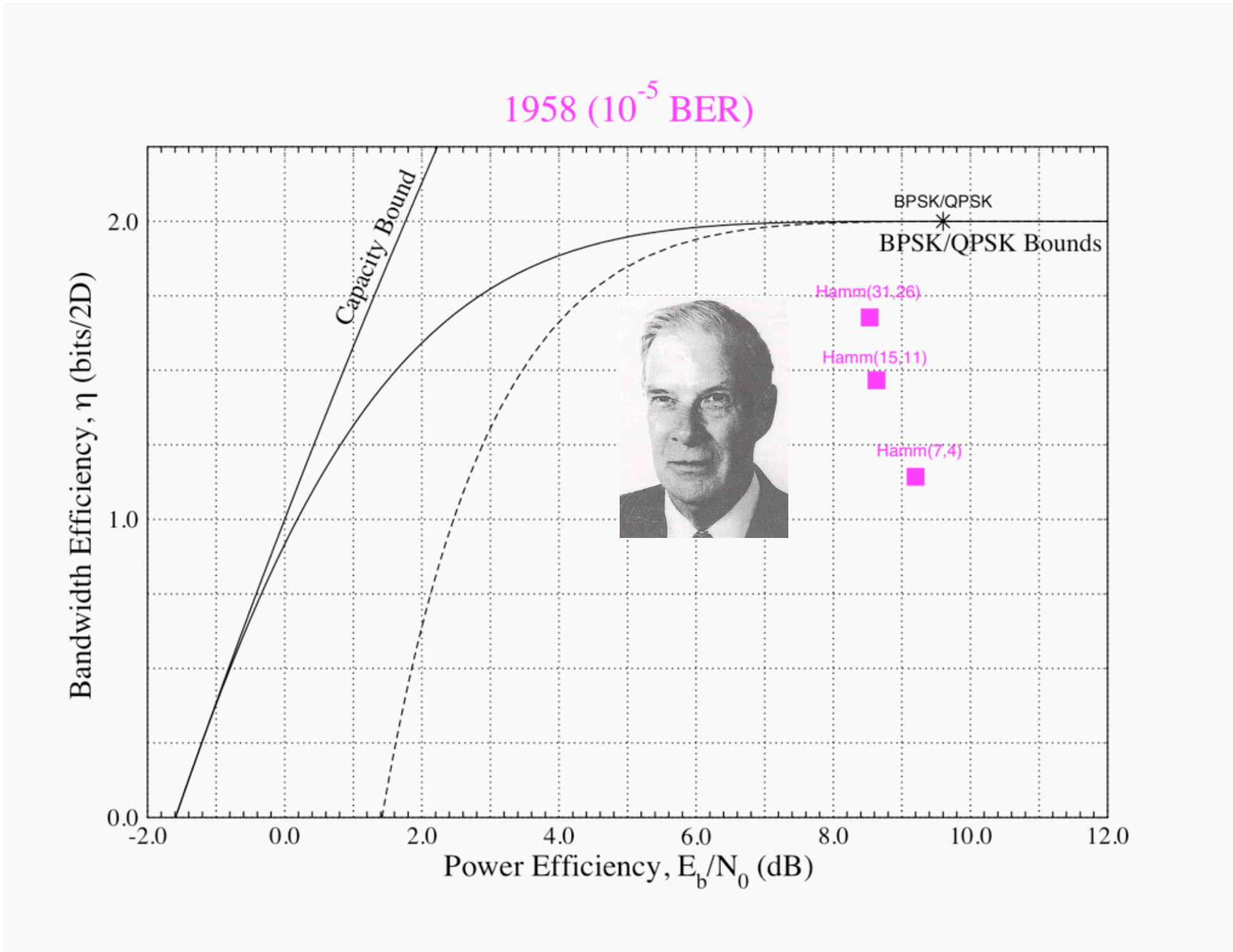
The First Day



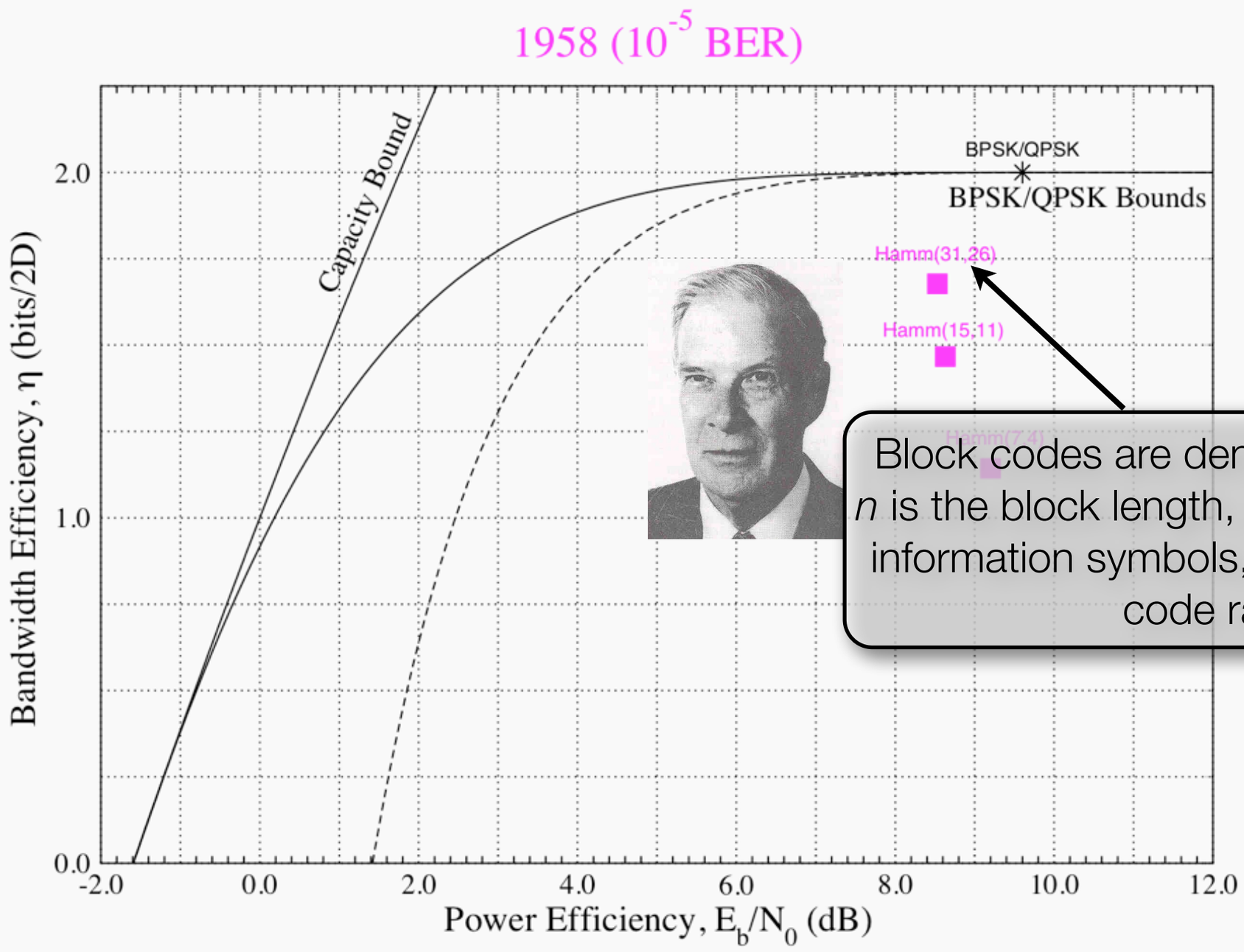
The First Day



The First Day

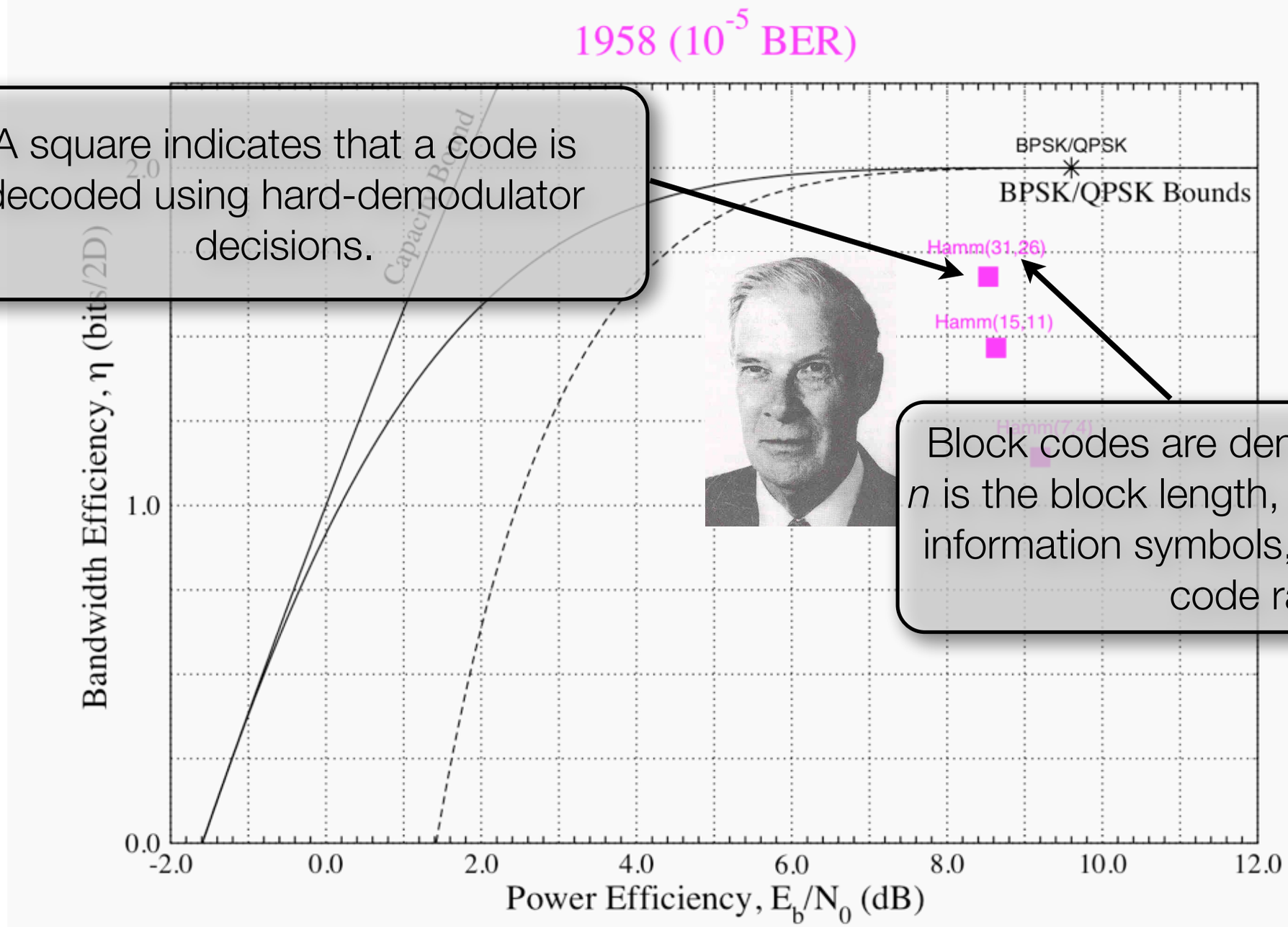


The First Day



Block codes are denoted (*n,k*), where *n* is the block length, *k* is the number of information symbols, and *R=k/n* is the code rate.

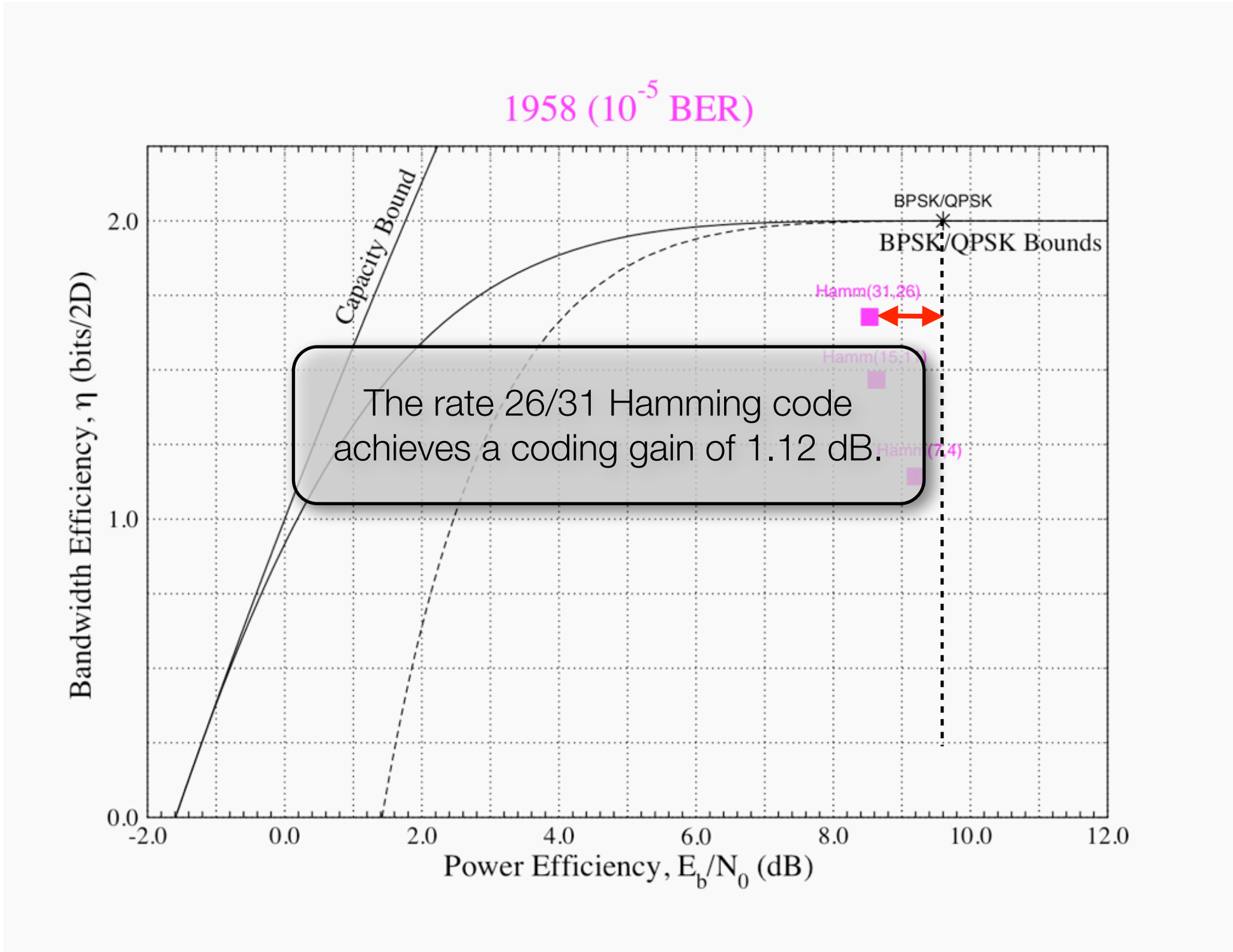
The First Day



A square indicates that a code is decoded using hard-demodulator decisions.

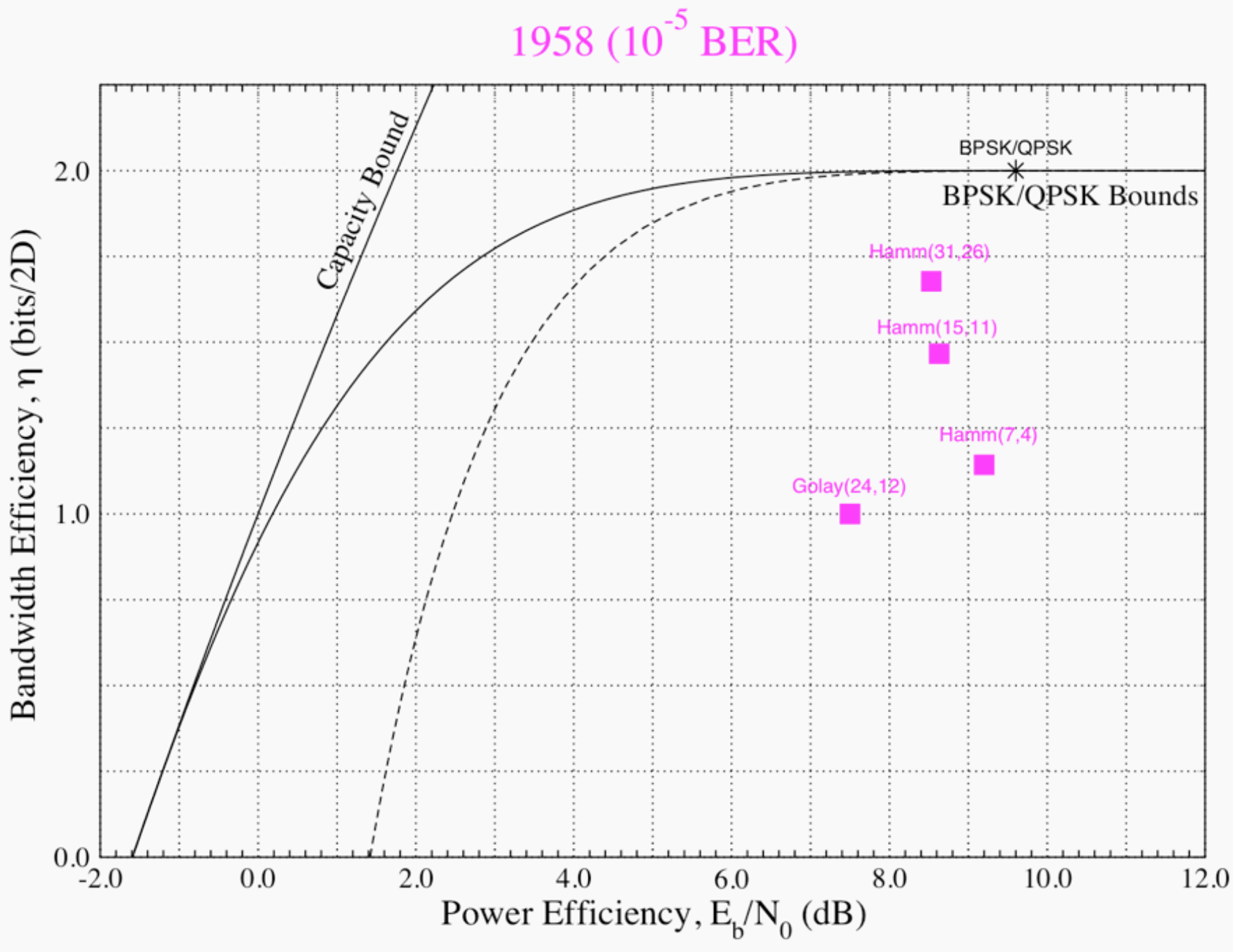
Block codes are denoted (*n,k*), where *n* is the block length, *k* is the number of information symbols, and *R=k/n* is the code rate.

The First Day

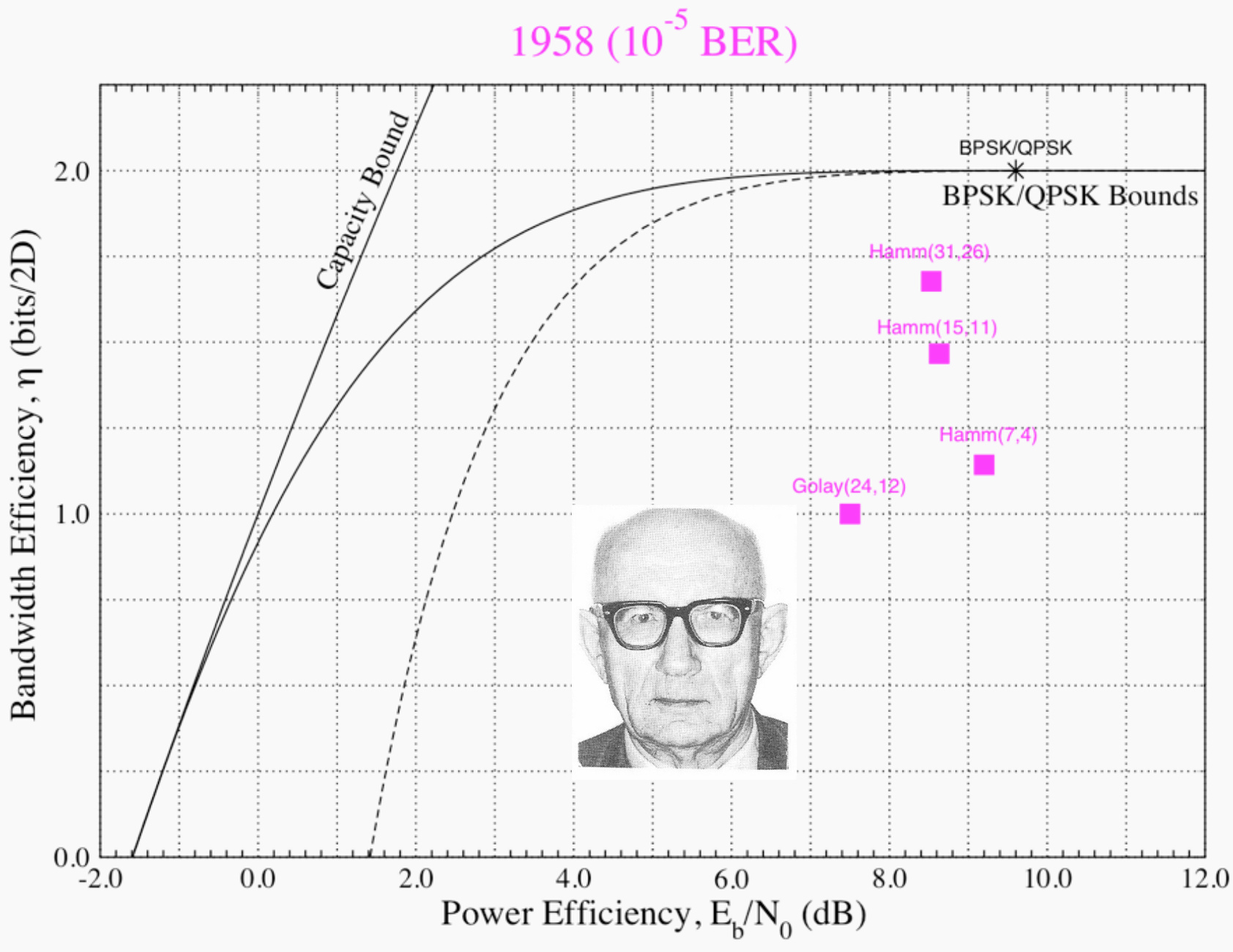


The rate 26/31 Hamming code achieves a coding gain of 1.12 dB.

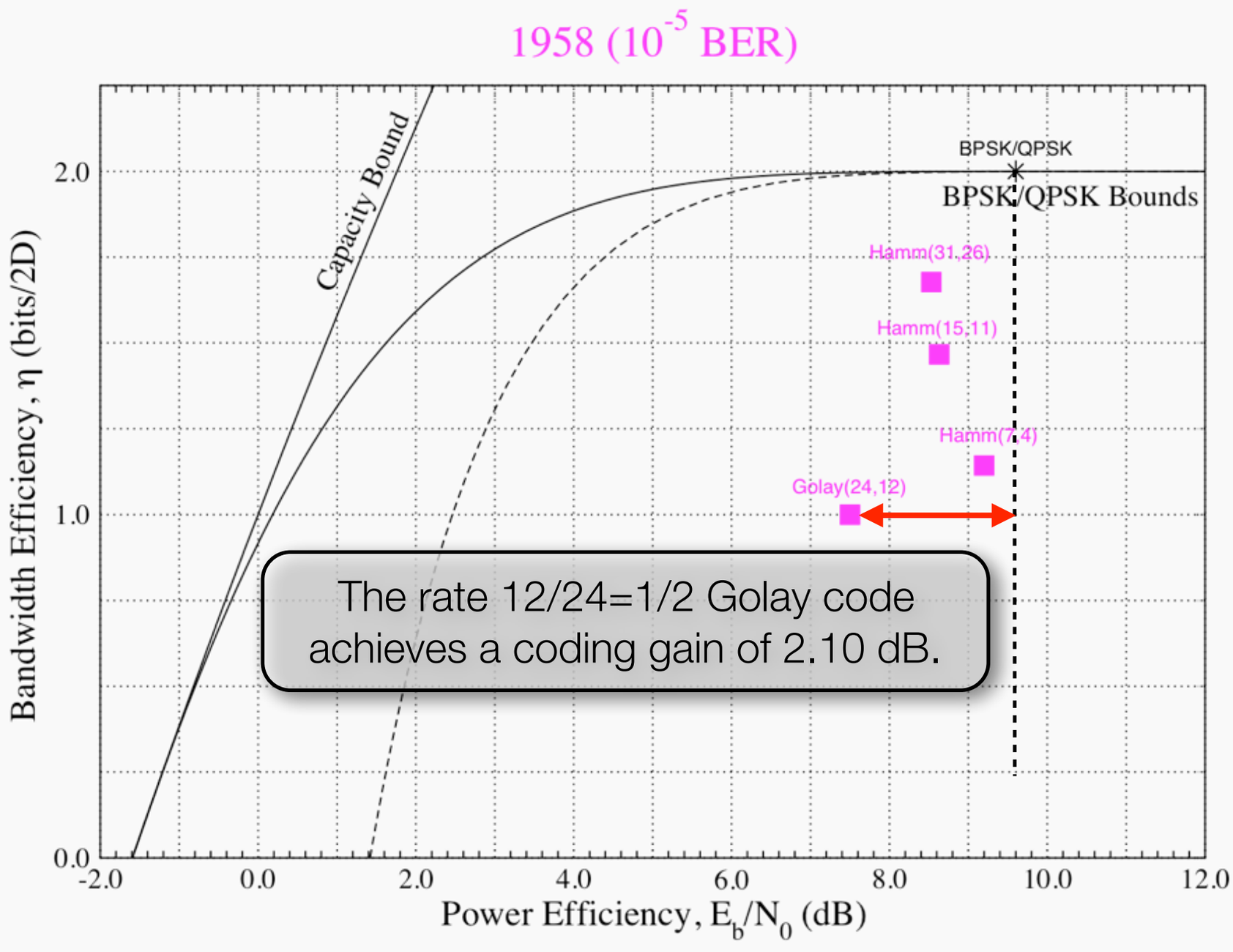
The First Day



The First Day

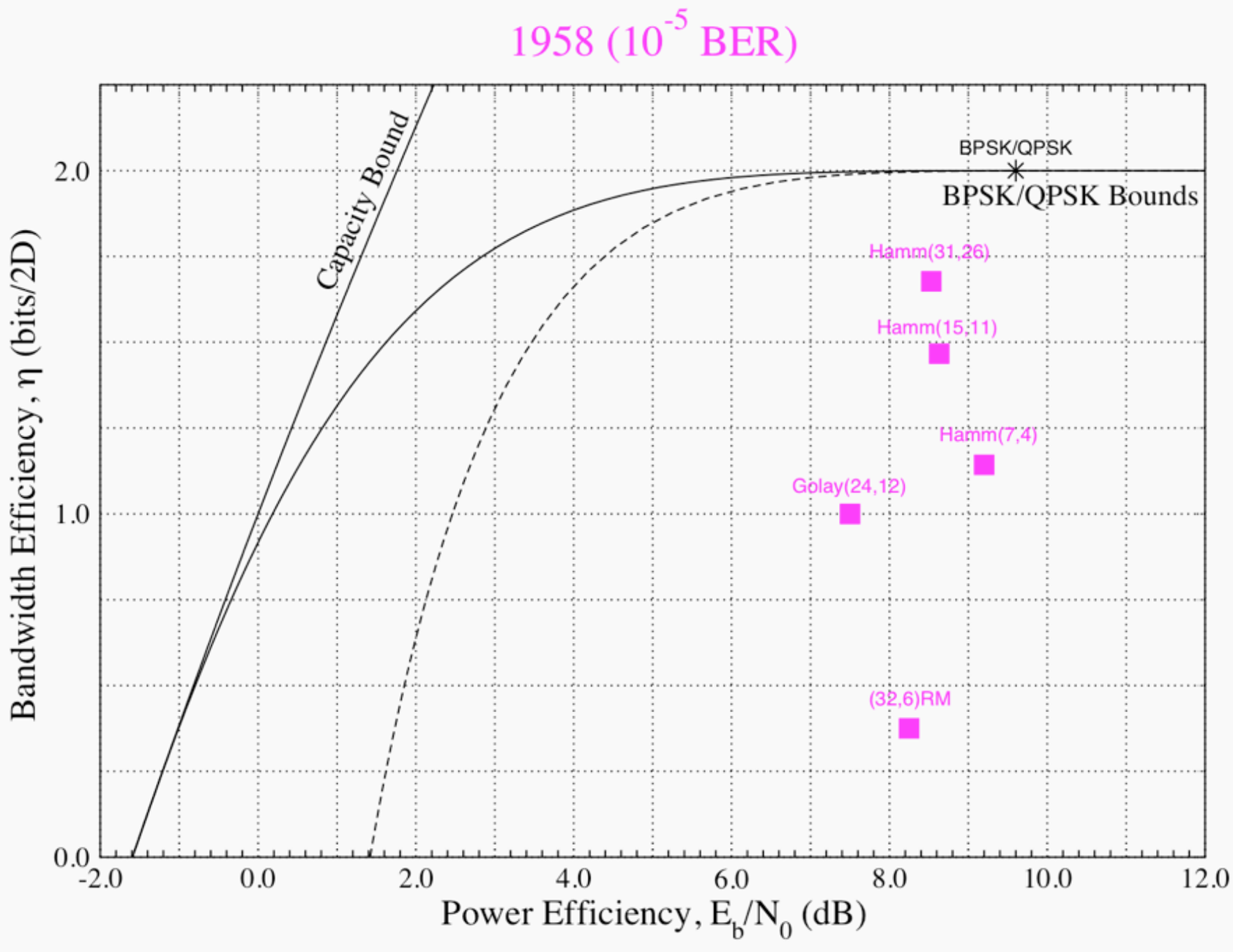


The First Day

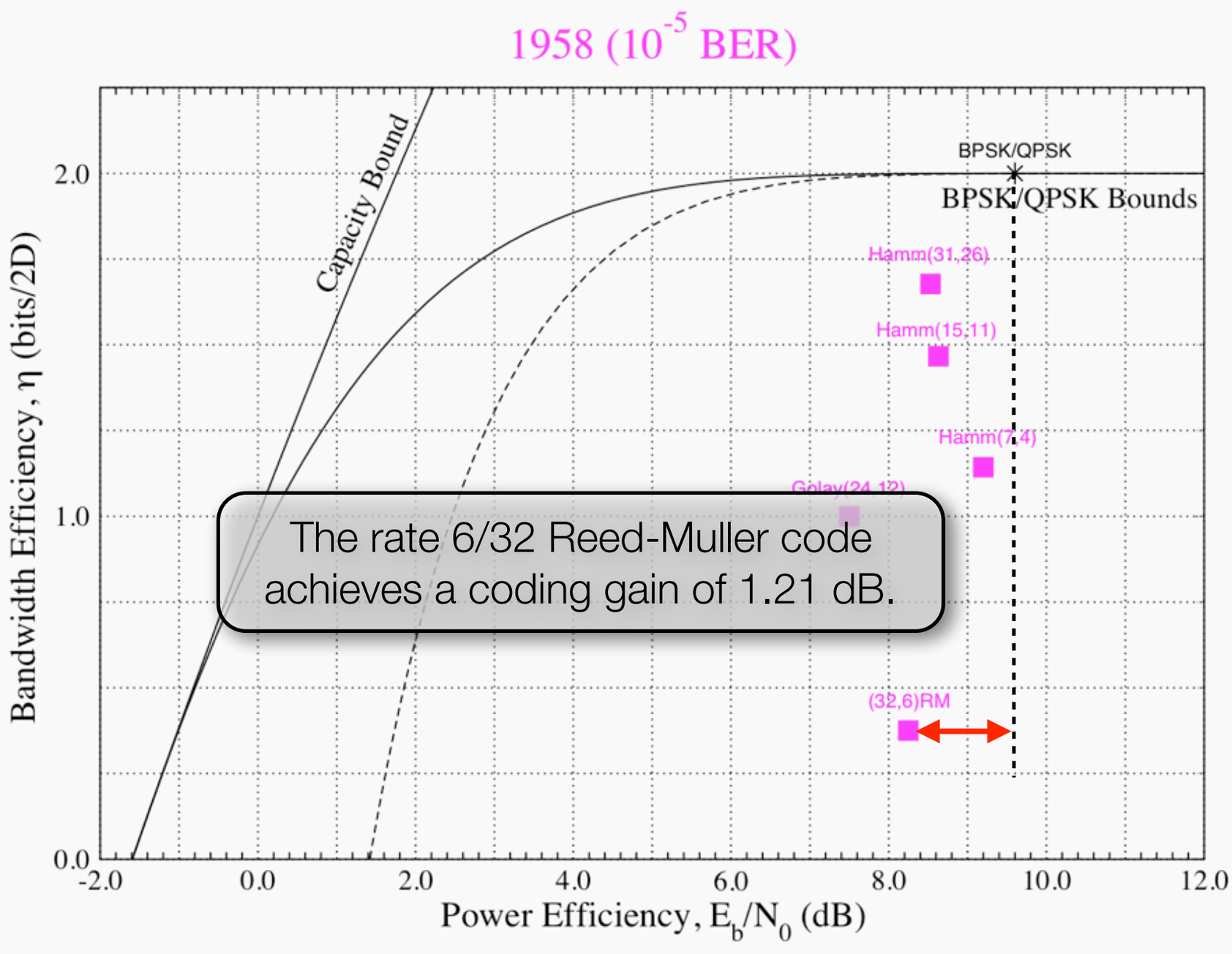


The rate 12/24=1/2 Golay code achieves a coding gain of 2.10 dB.

The First Day

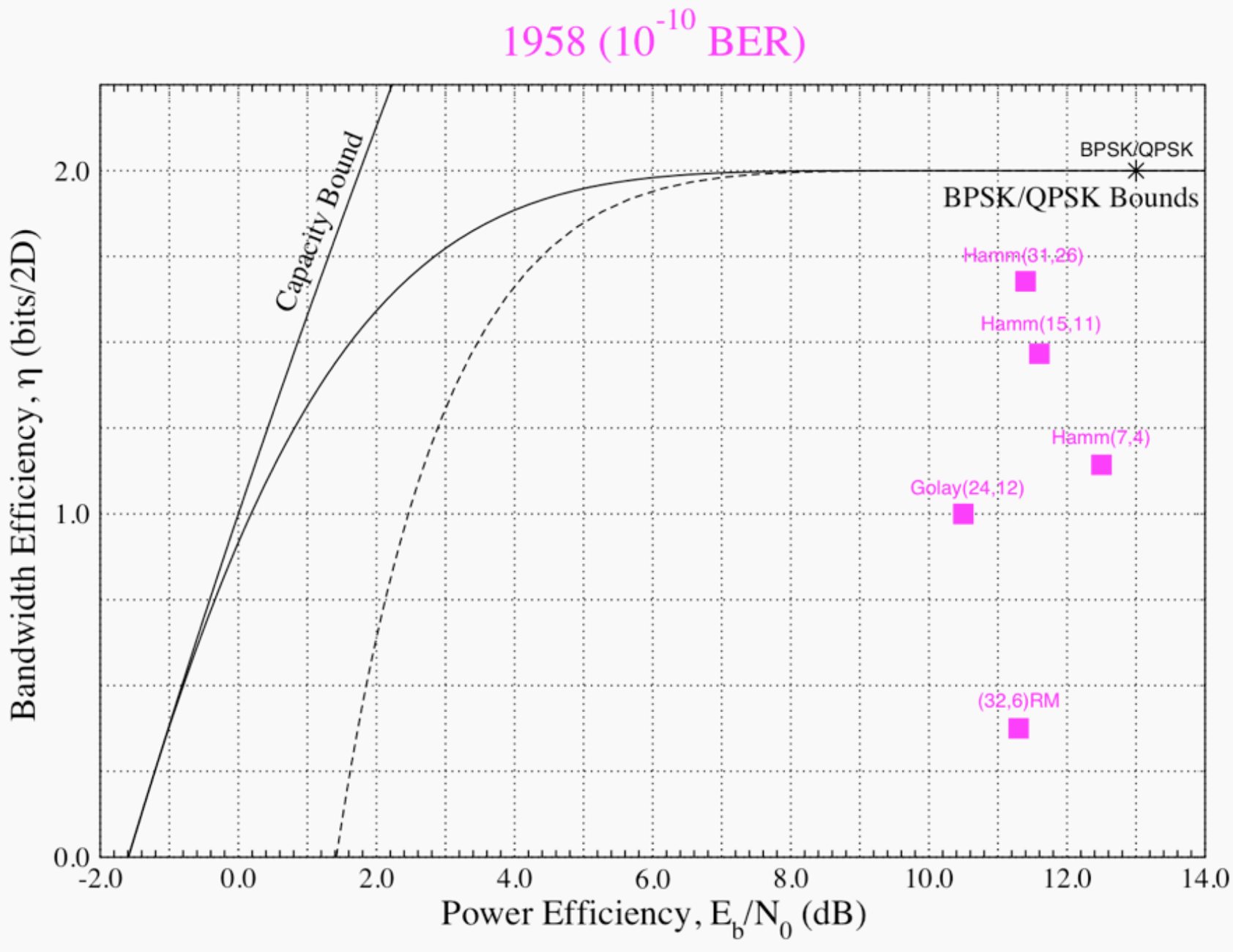


The First Day

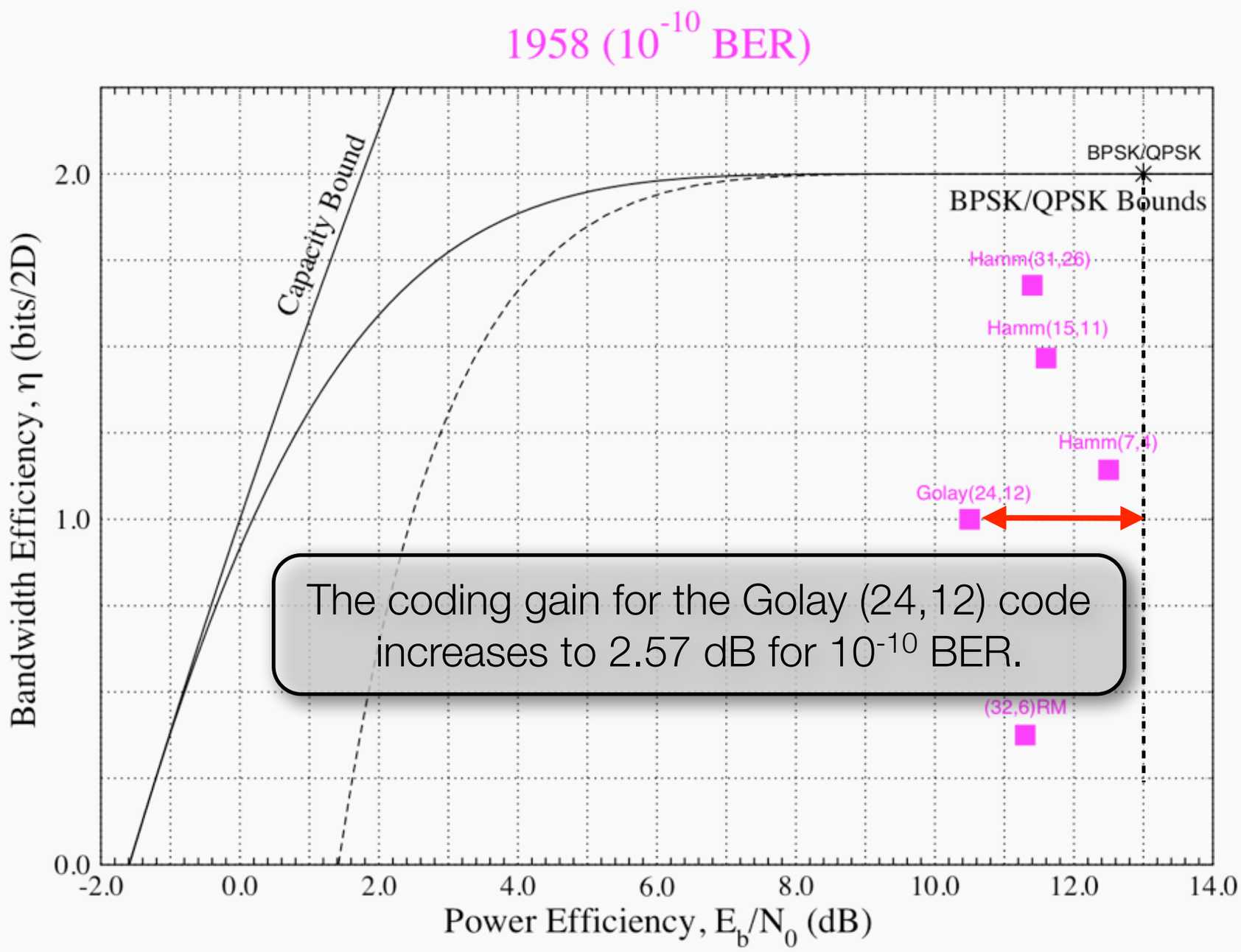


The rate 6/32 Reed-Muller code achieves a coding gain of 1.21 dB.

The First Day



The First Day

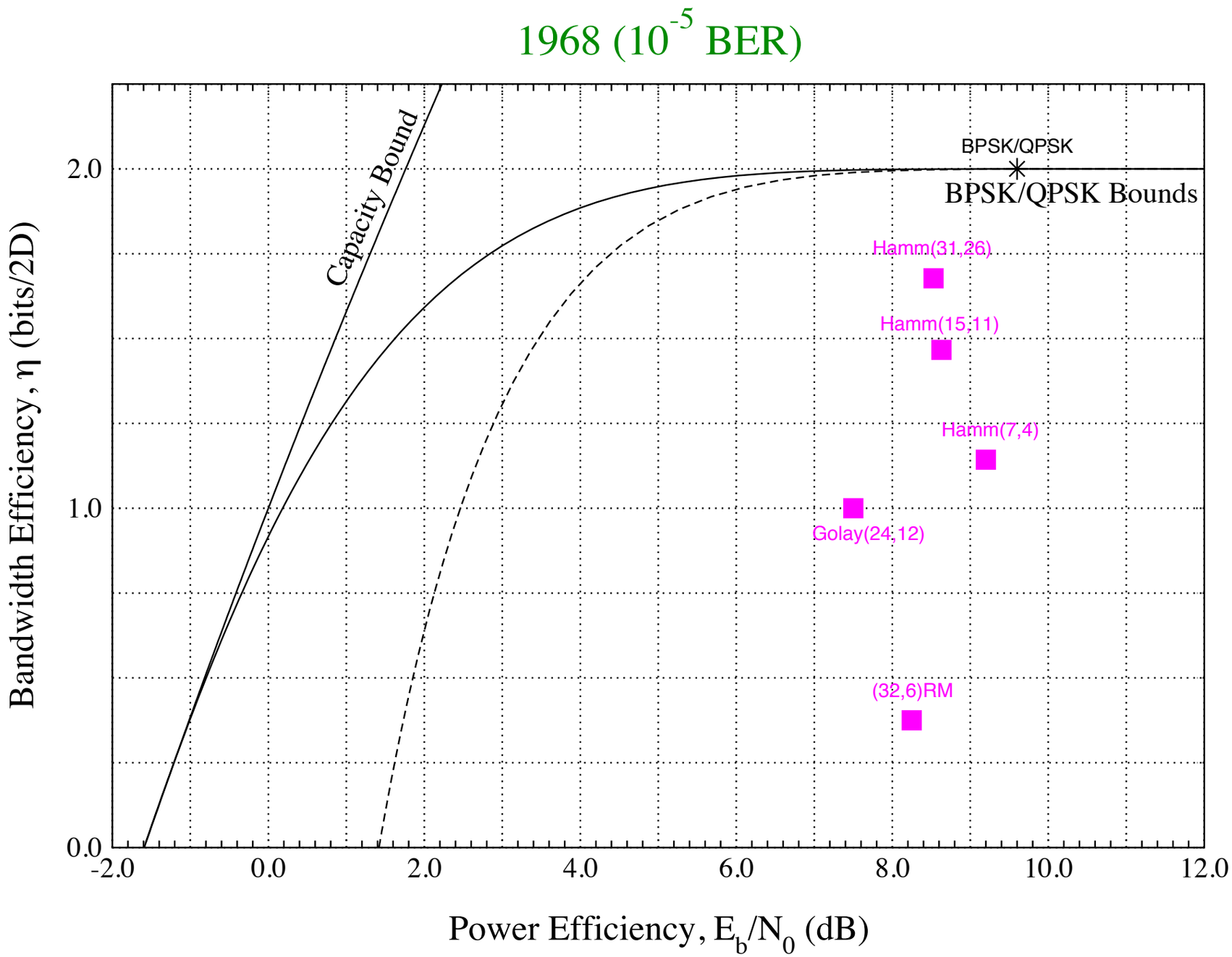


The coding gain for the Golay (24,12) code increases to 2.57 dB for 10^{-10} BER.

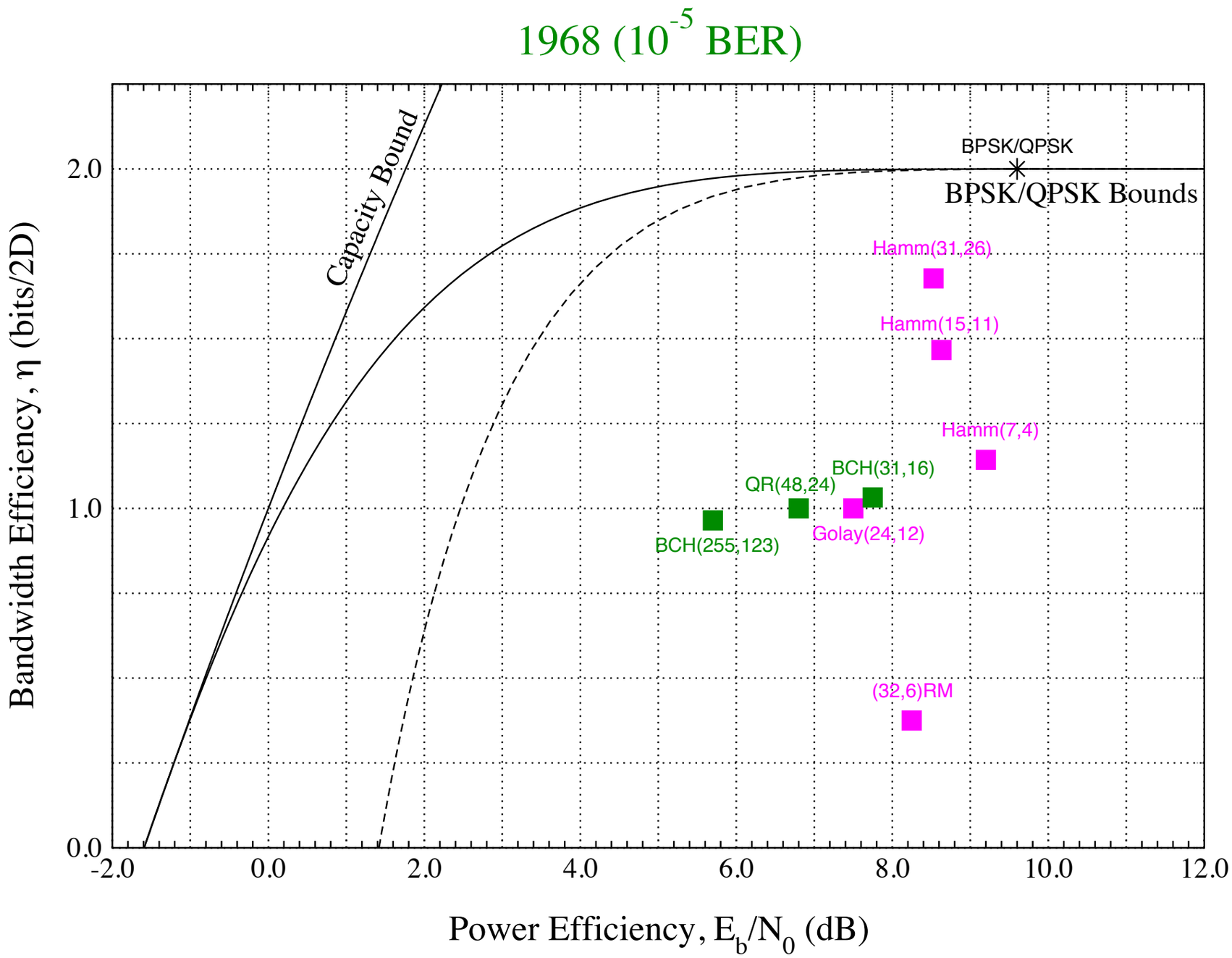
The Second Day

The Second Day

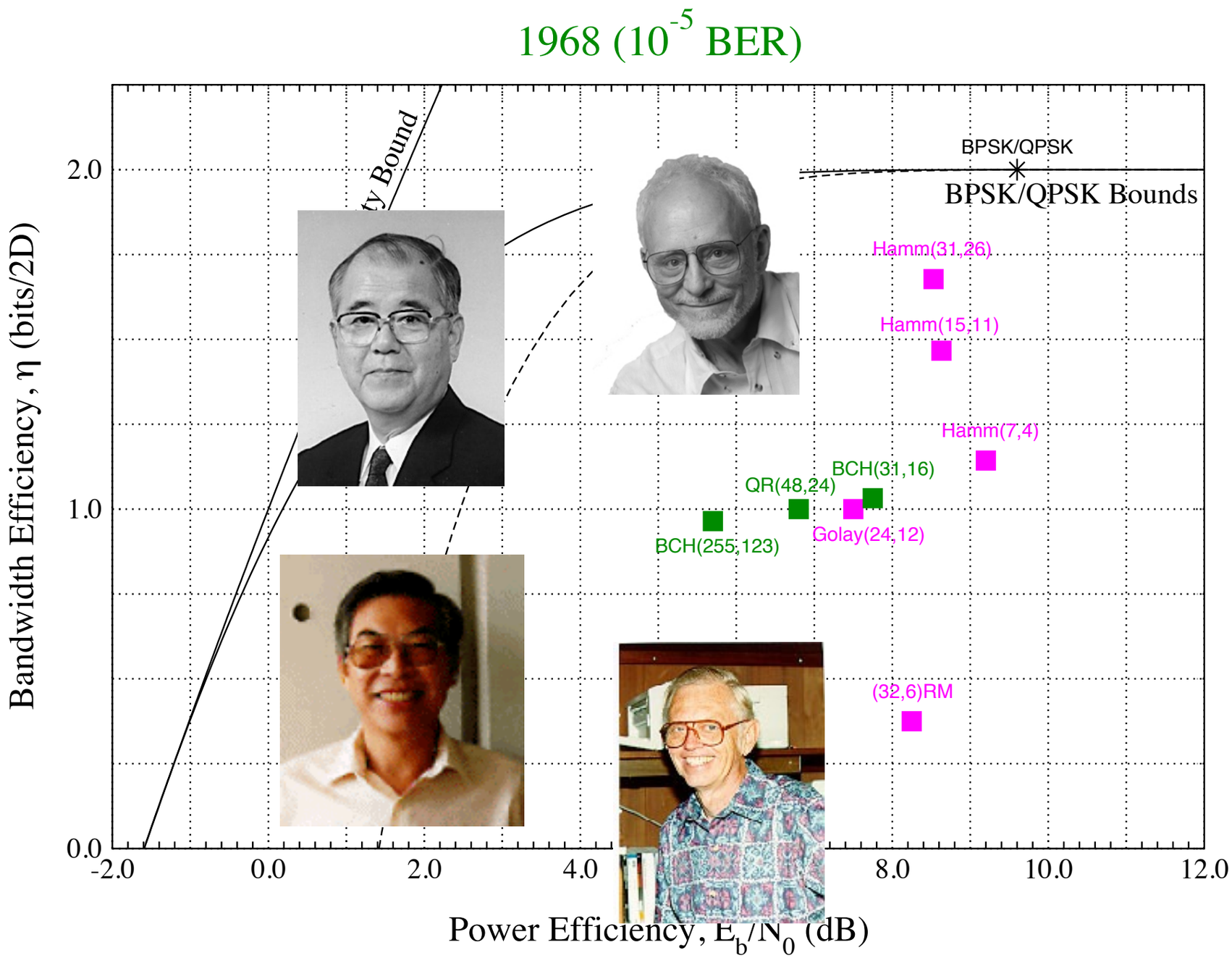
The Second Day



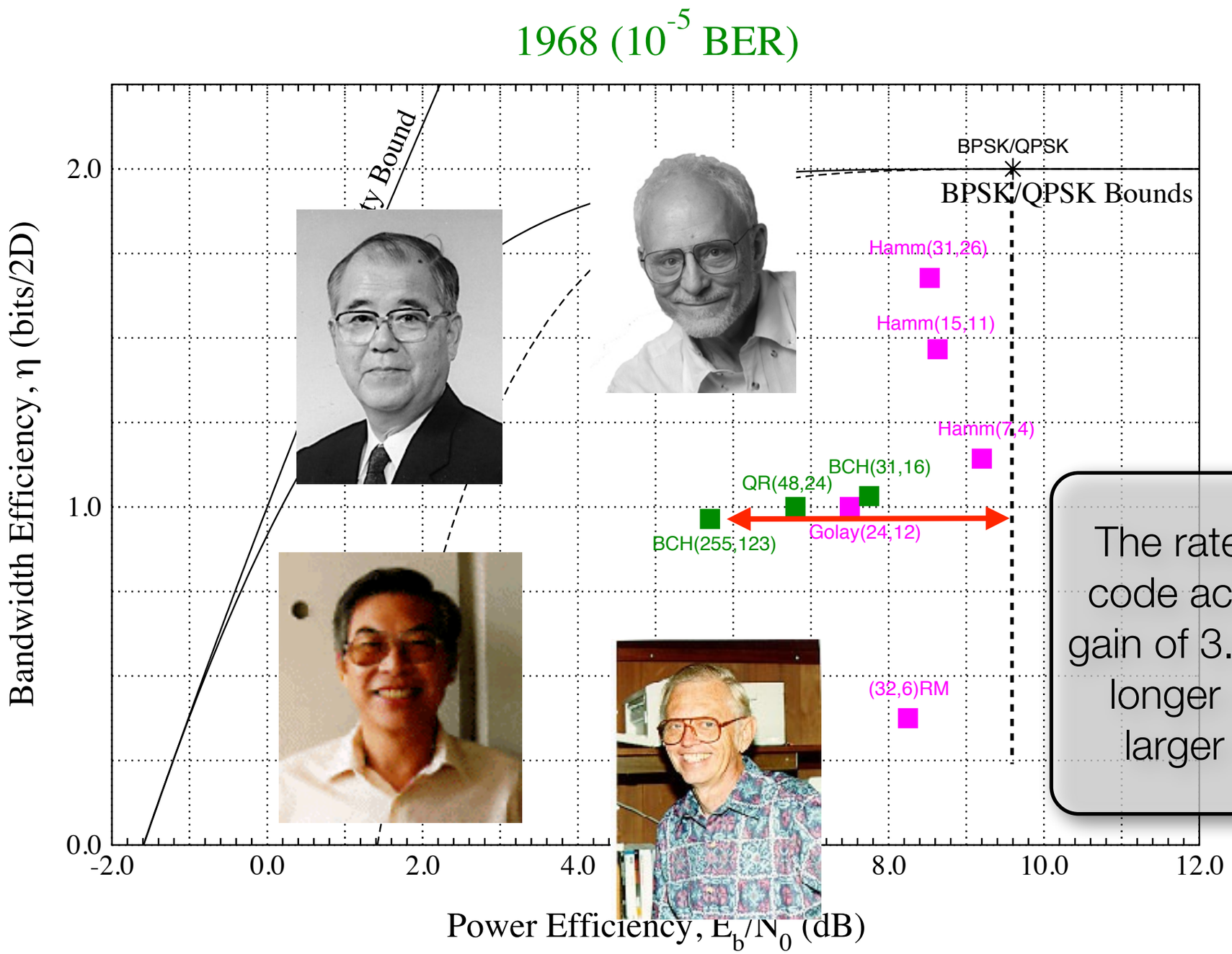
The Second Day



The Second Day

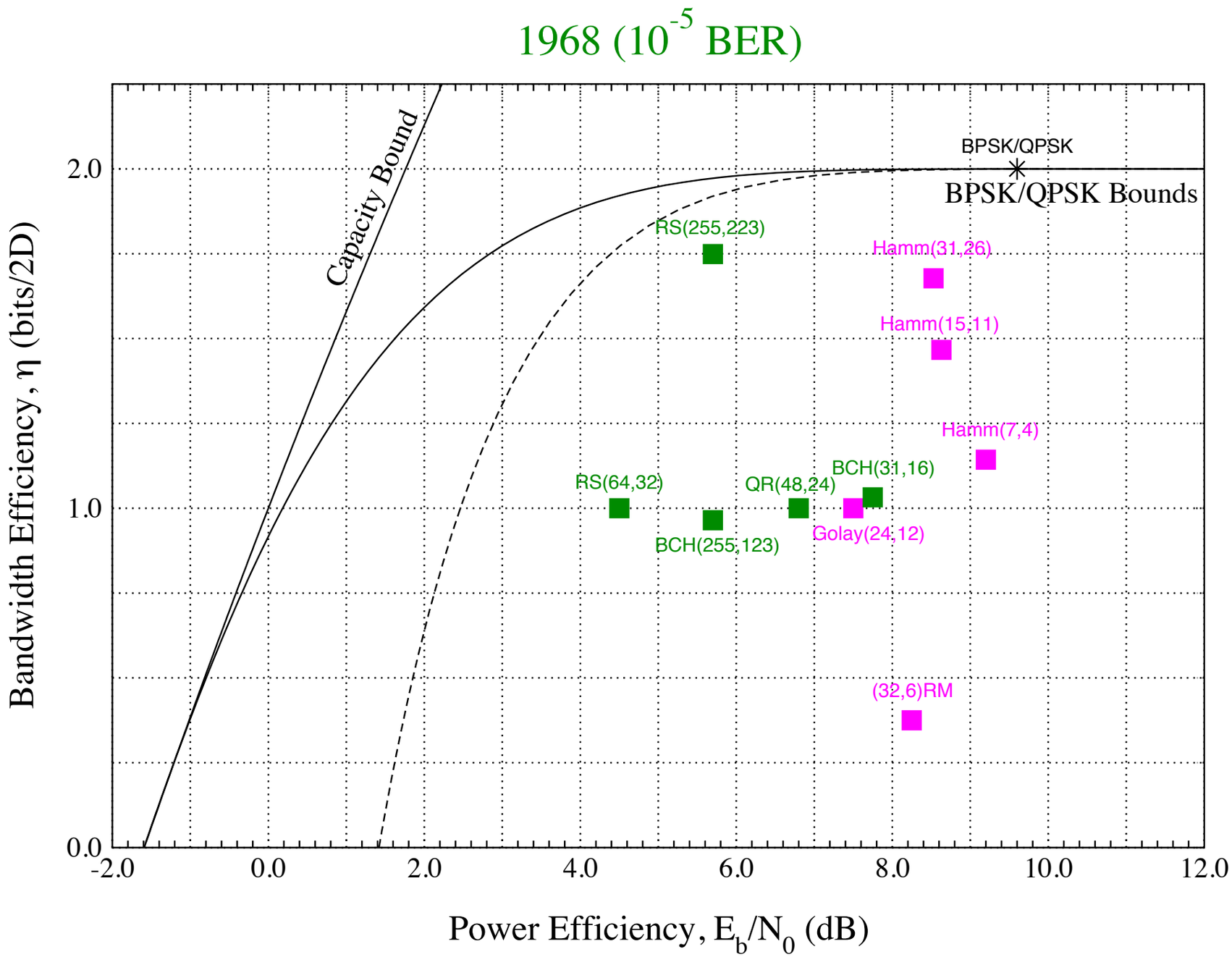


The Second Day

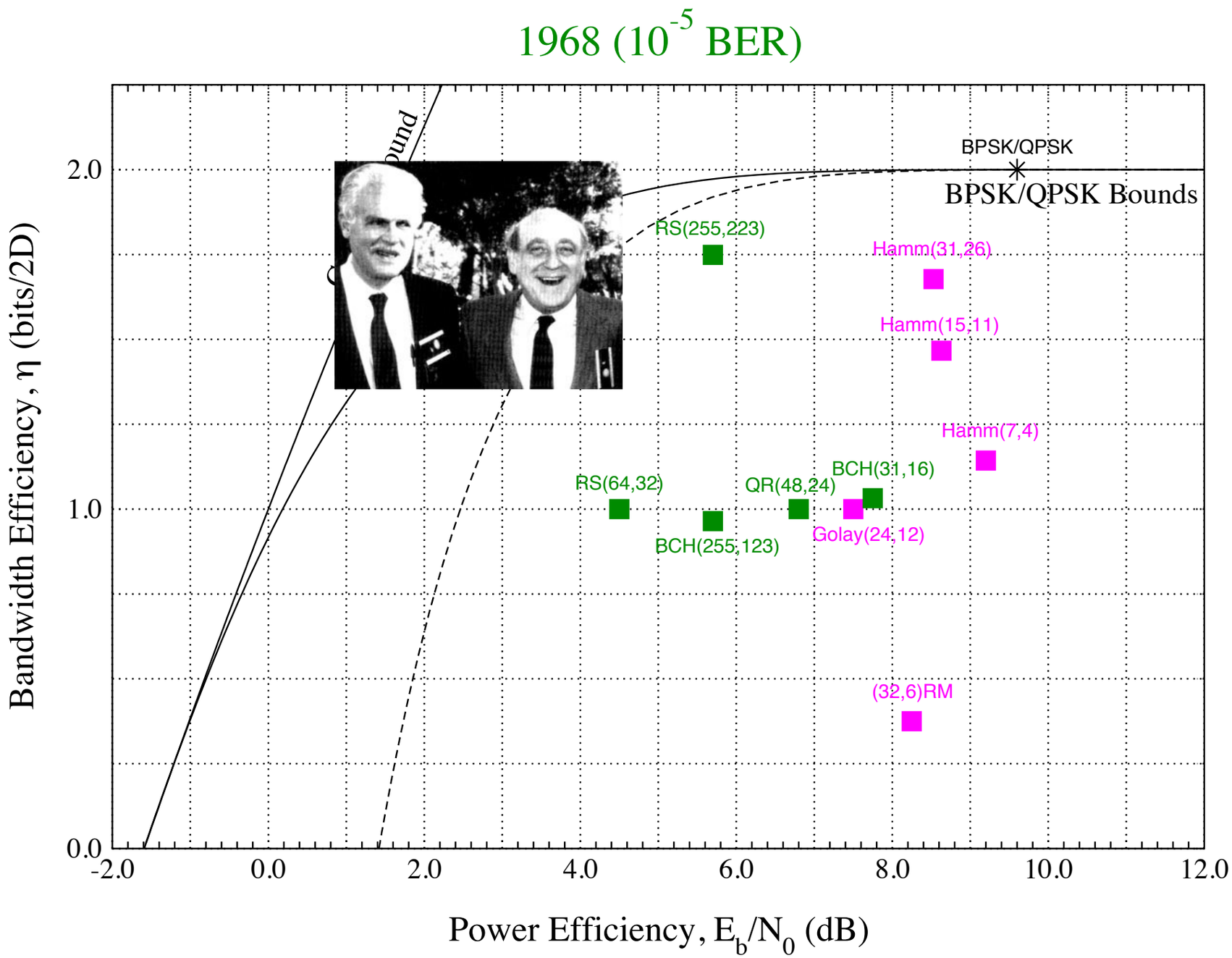


The rate 123/255 BCH code achieves a coding gain of 3.61 dB. Note that longer codes achieve larger coding gains.

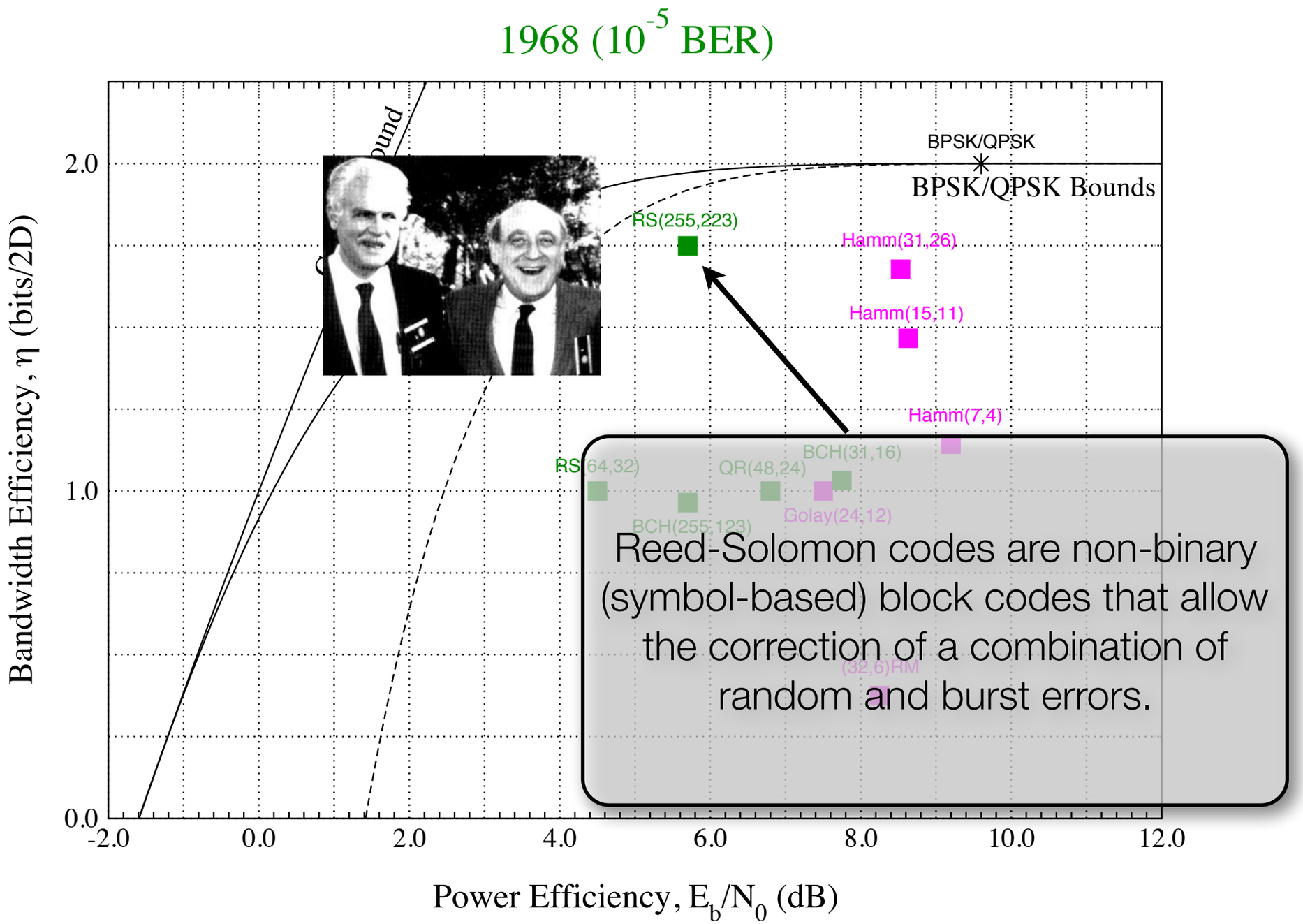
The Second Day



The Second Day

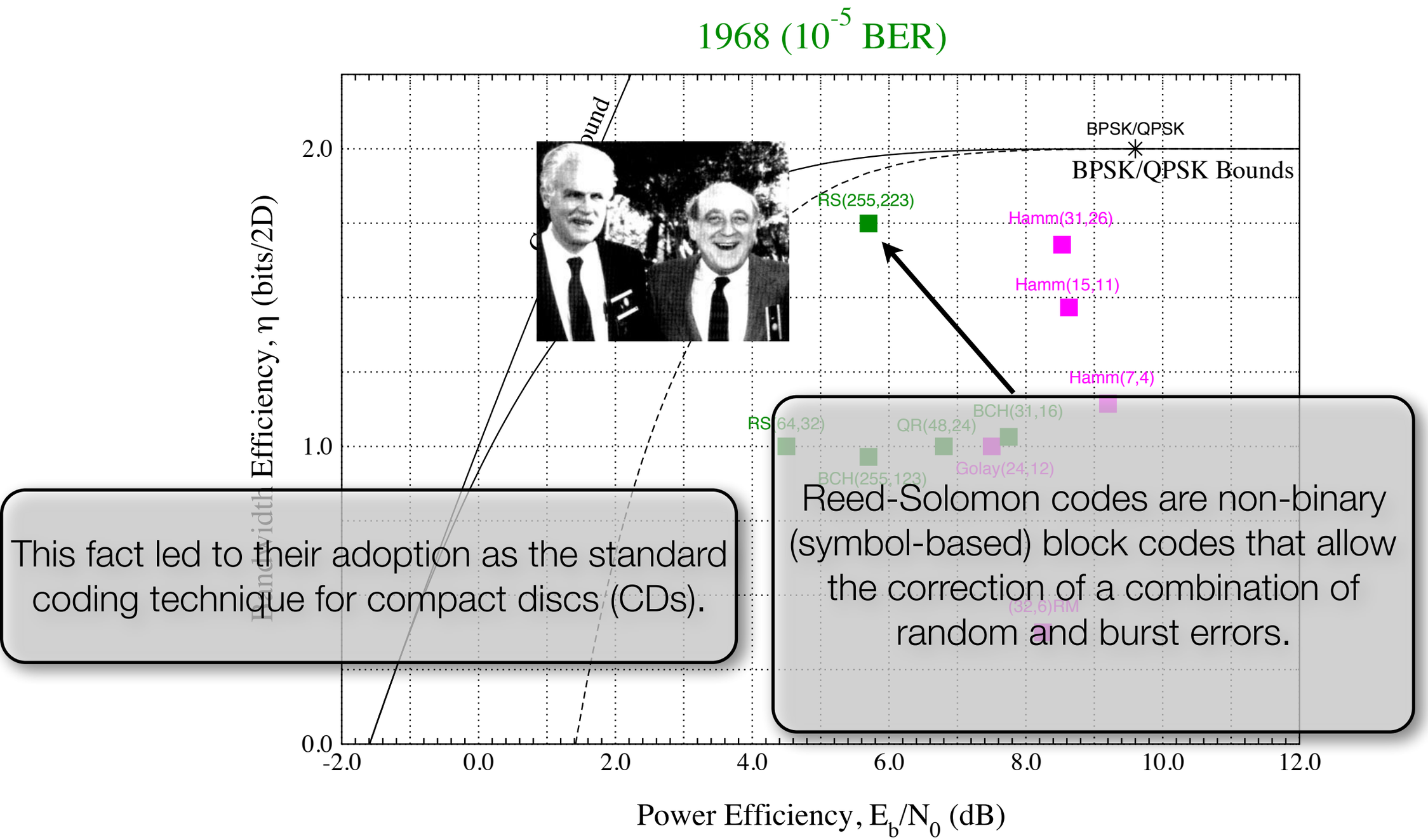


The Second Day



Reed-Solomon codes are non-binary (symbol-based) block codes that allow the correction of a combination of random and burst errors.

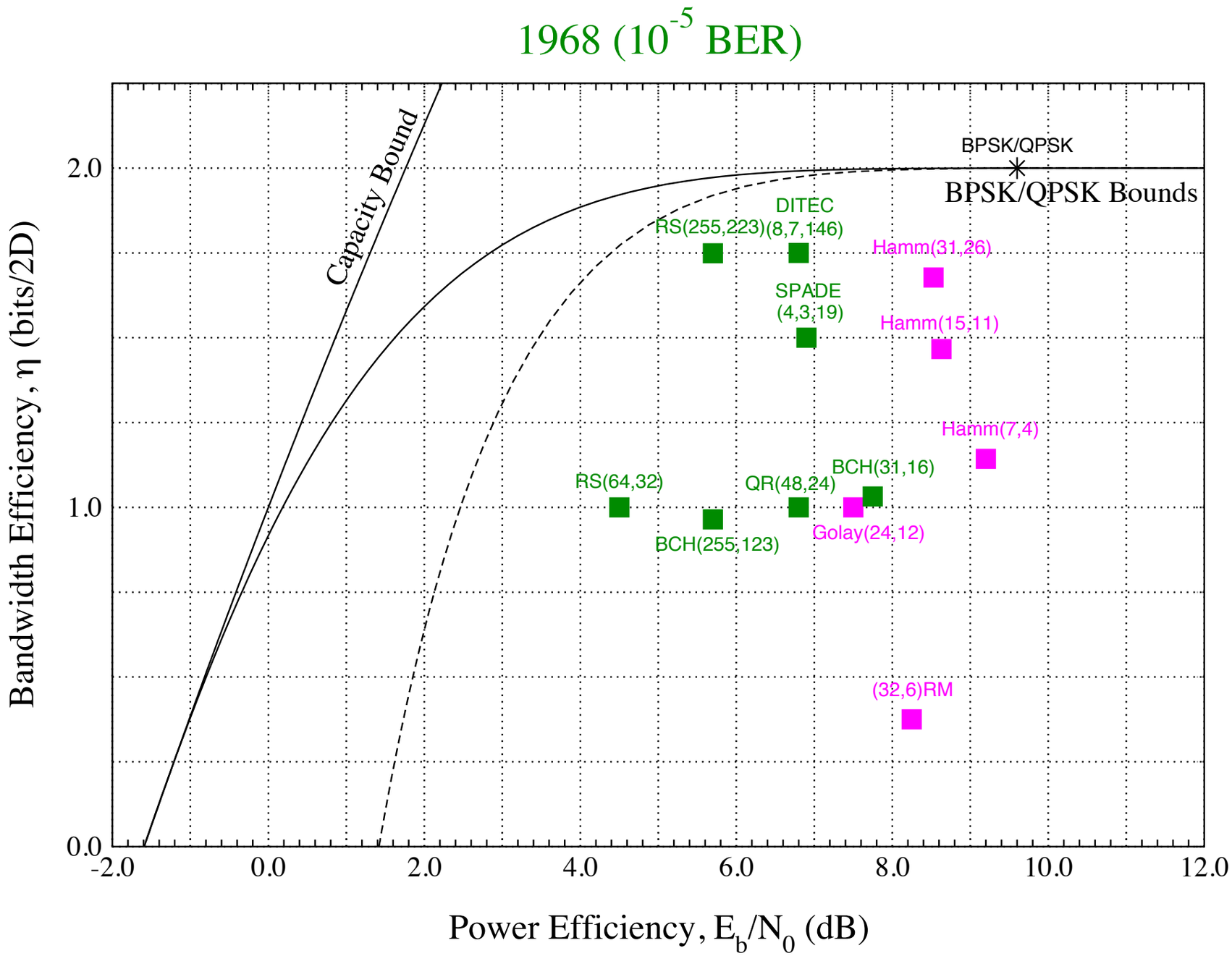
The Second Day



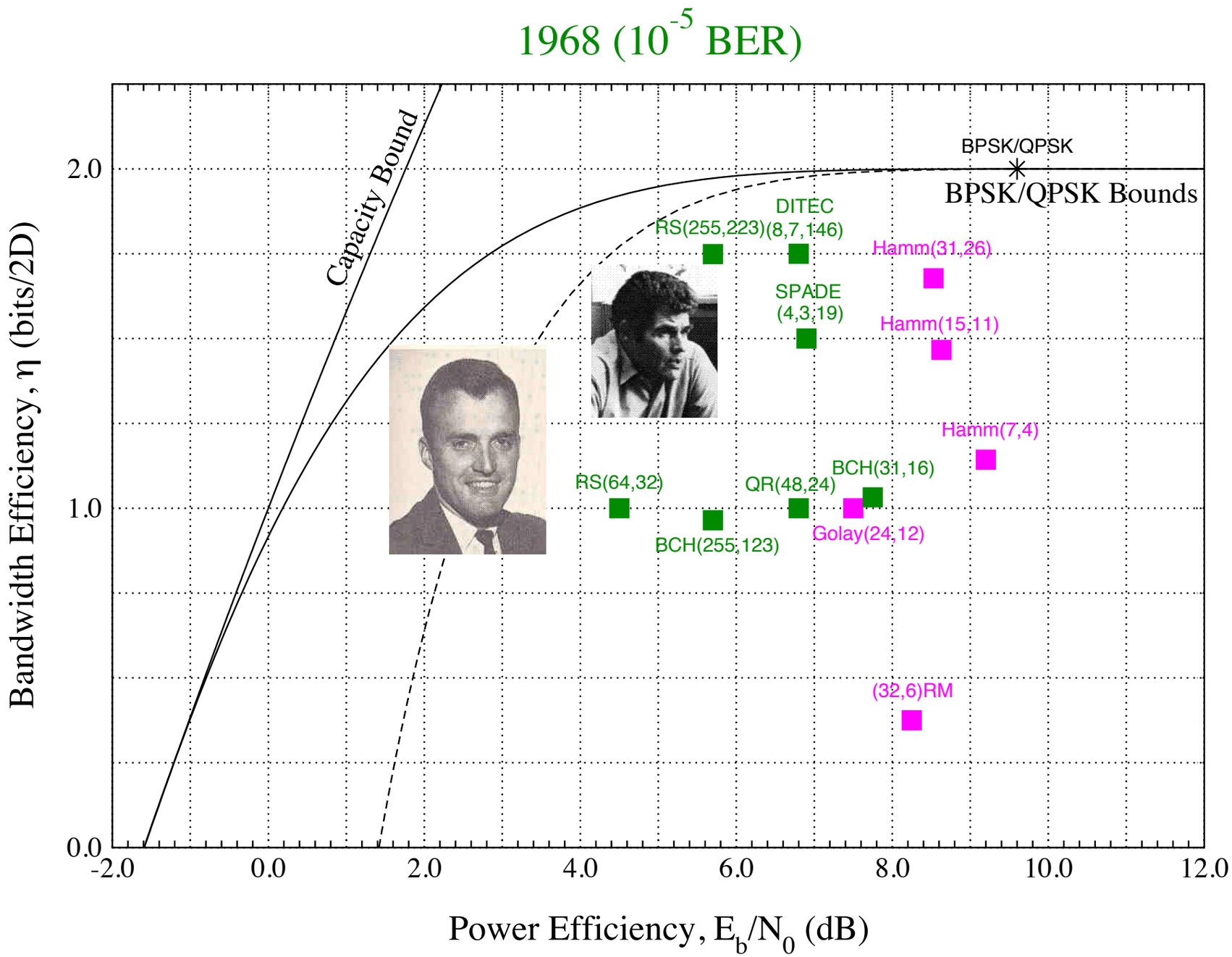
This fact led to their adoption as the standard coding technique for compact discs (CDs).

Reed-Solomon codes are non-binary (symbol-based) block codes that allow the correction of a combination of random and burst errors.

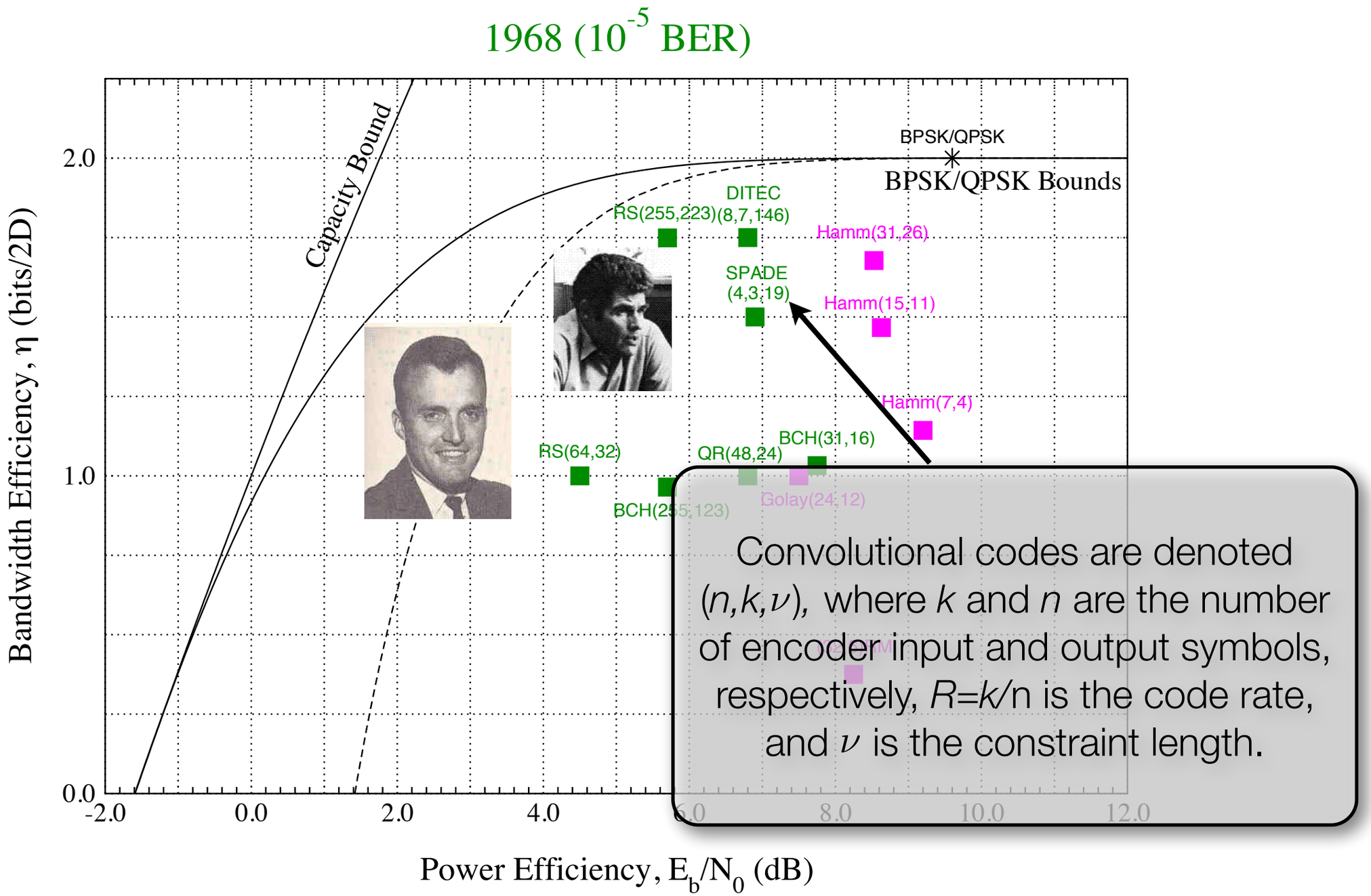
The Second Day



The Second Day

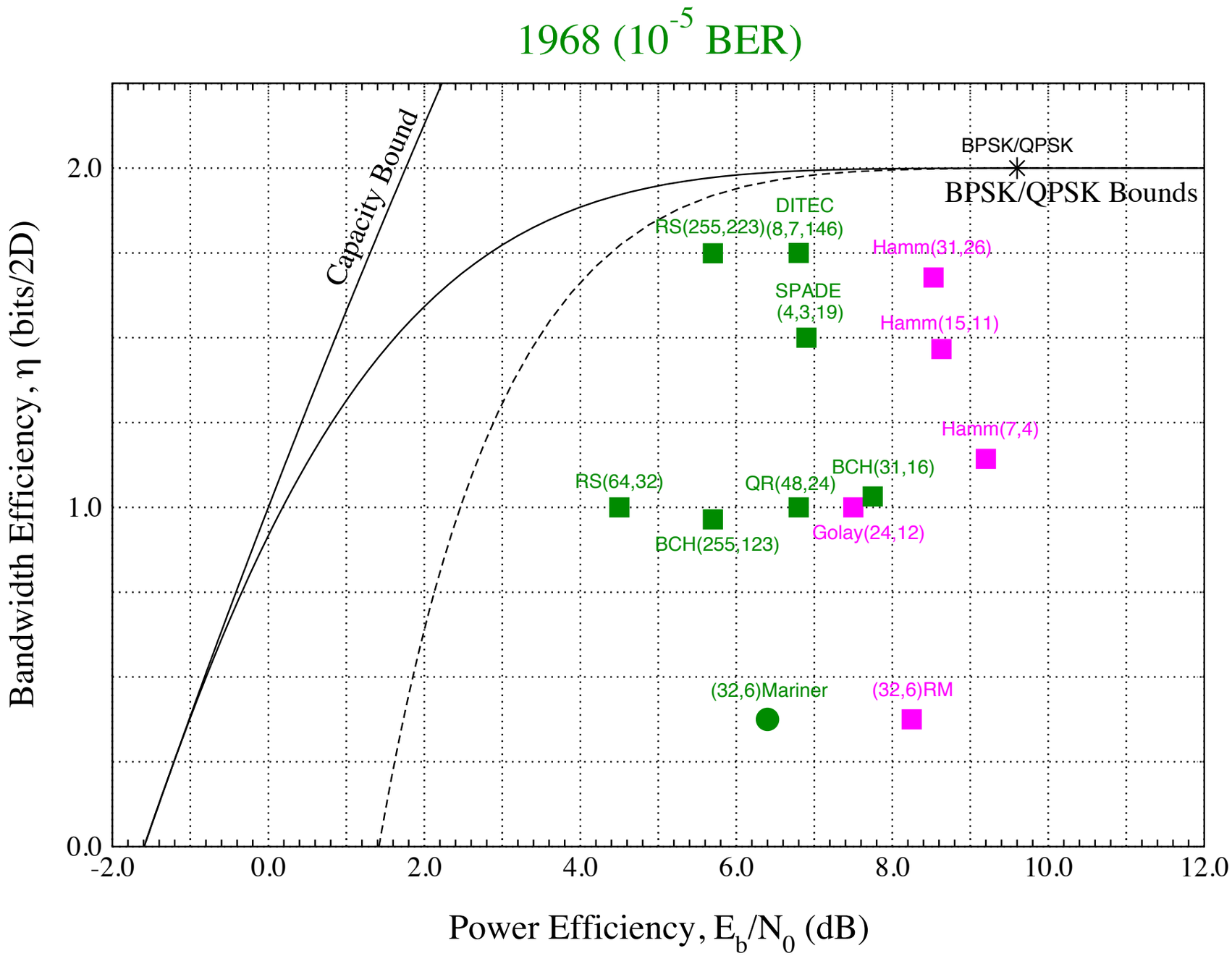


The Second Day

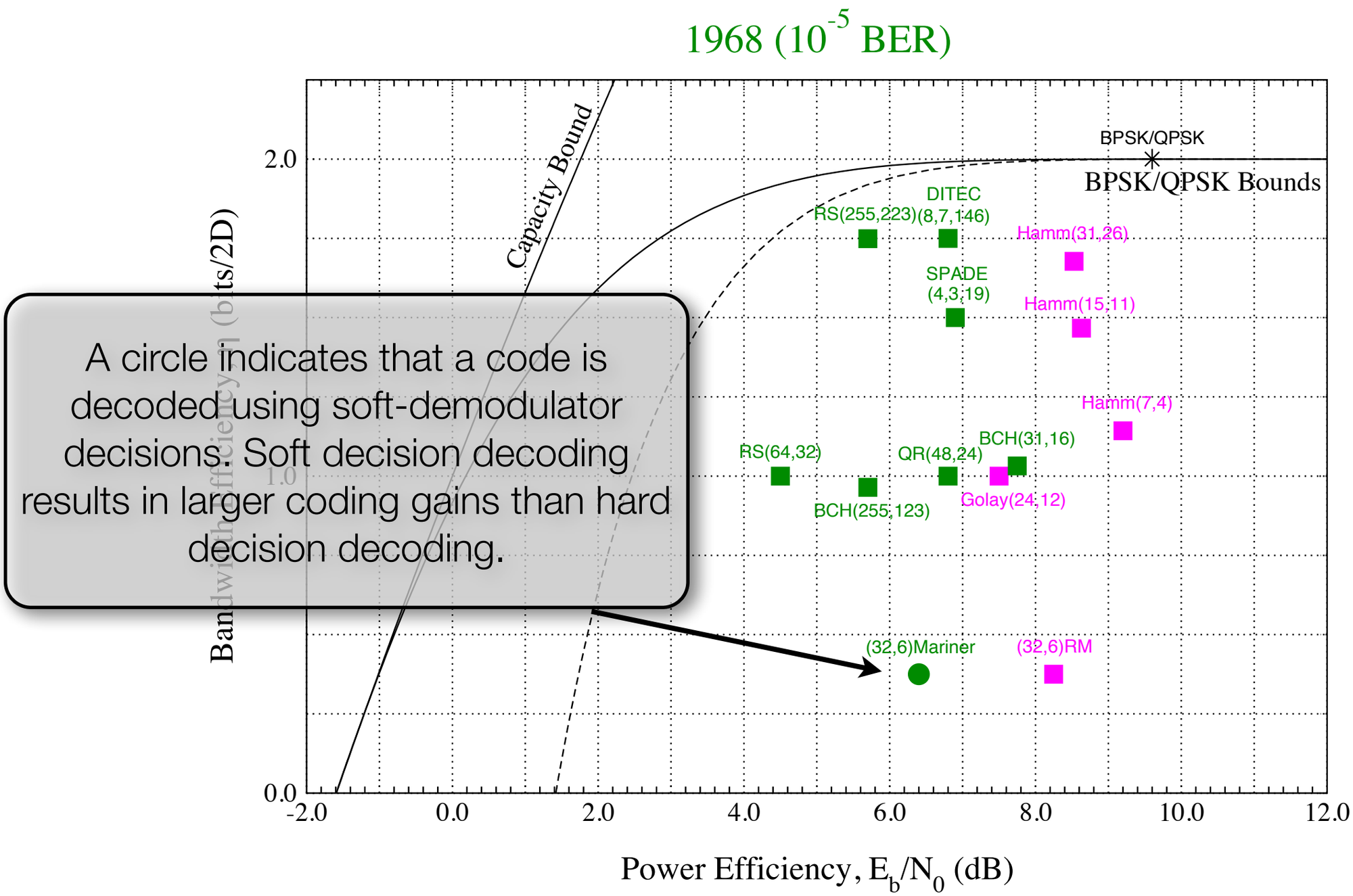


Convolutional codes are denoted (n,k,ν), where k and n are the number of encoder input and output symbols, respectively, $R=k/n$ is the code rate, and ν is the constraint length.

The Second Day

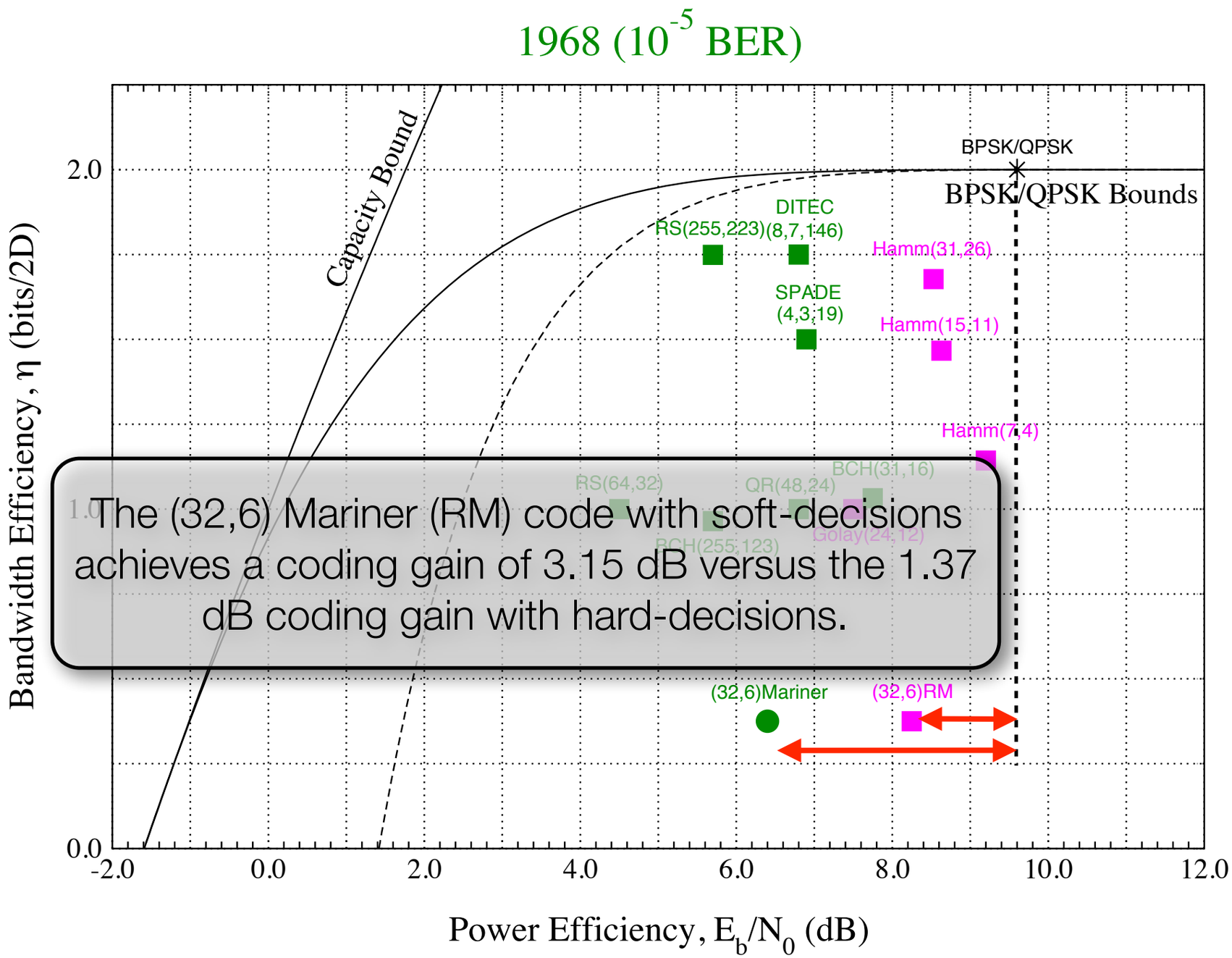


The Second Day



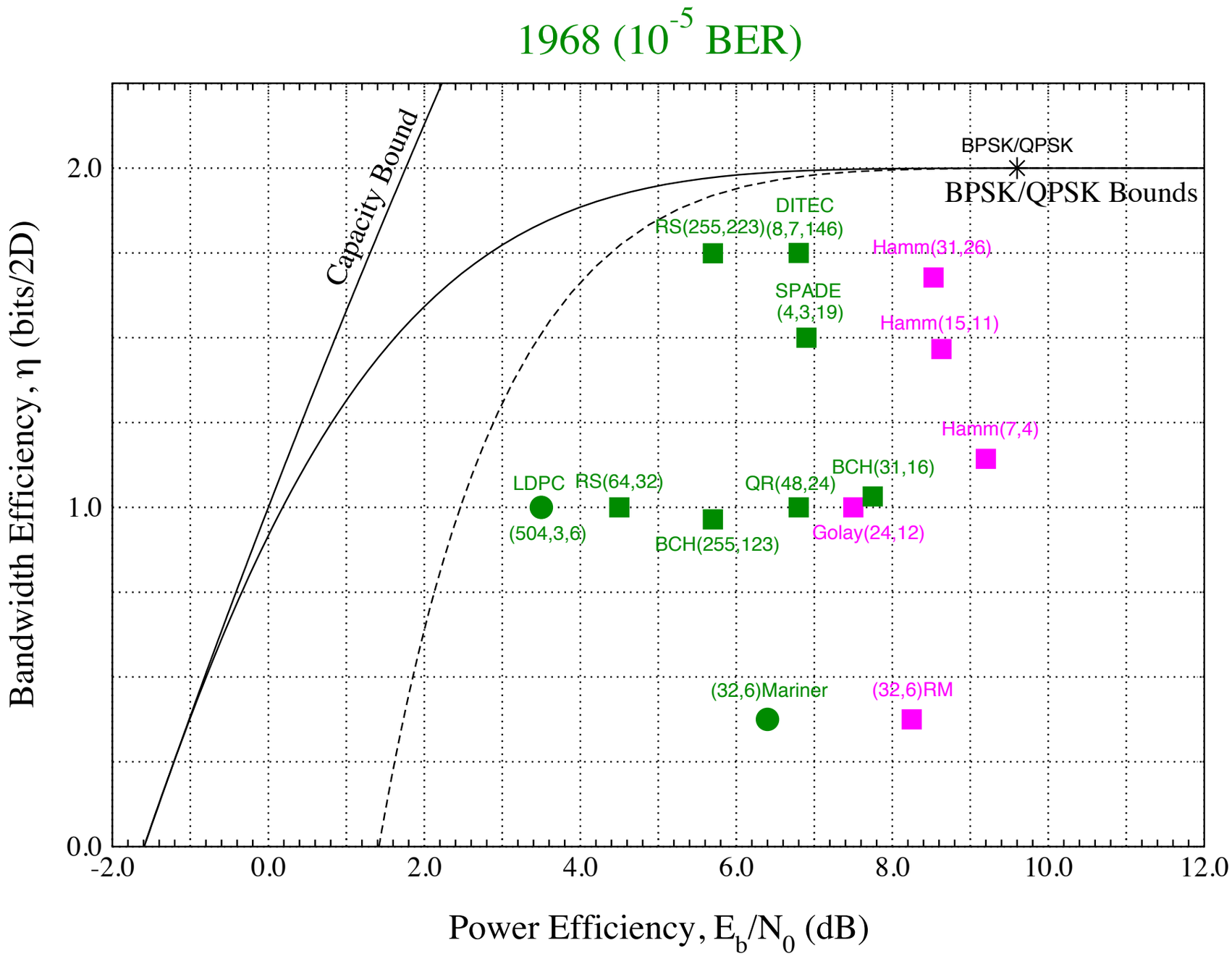
A circle indicates that a code is decoded using soft-demodulator decisions. Soft decision decoding results in larger coding gains than hard decision decoding.

The Second Day

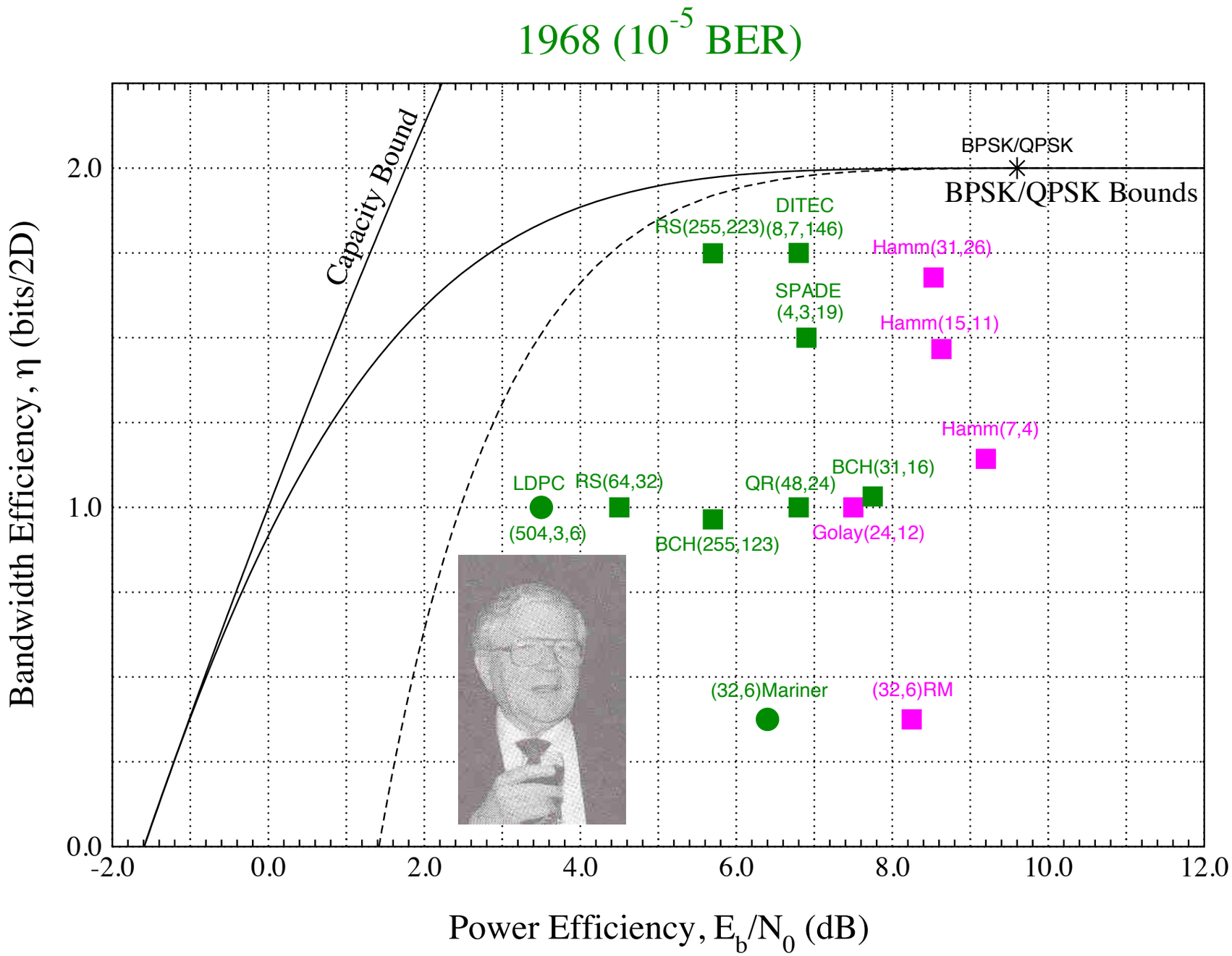


The (32,6) Mariner (RM) code with soft-decisions achieves a coding gain of 3.15 dB versus the 1.37 dB coding gain with hard-decisions.

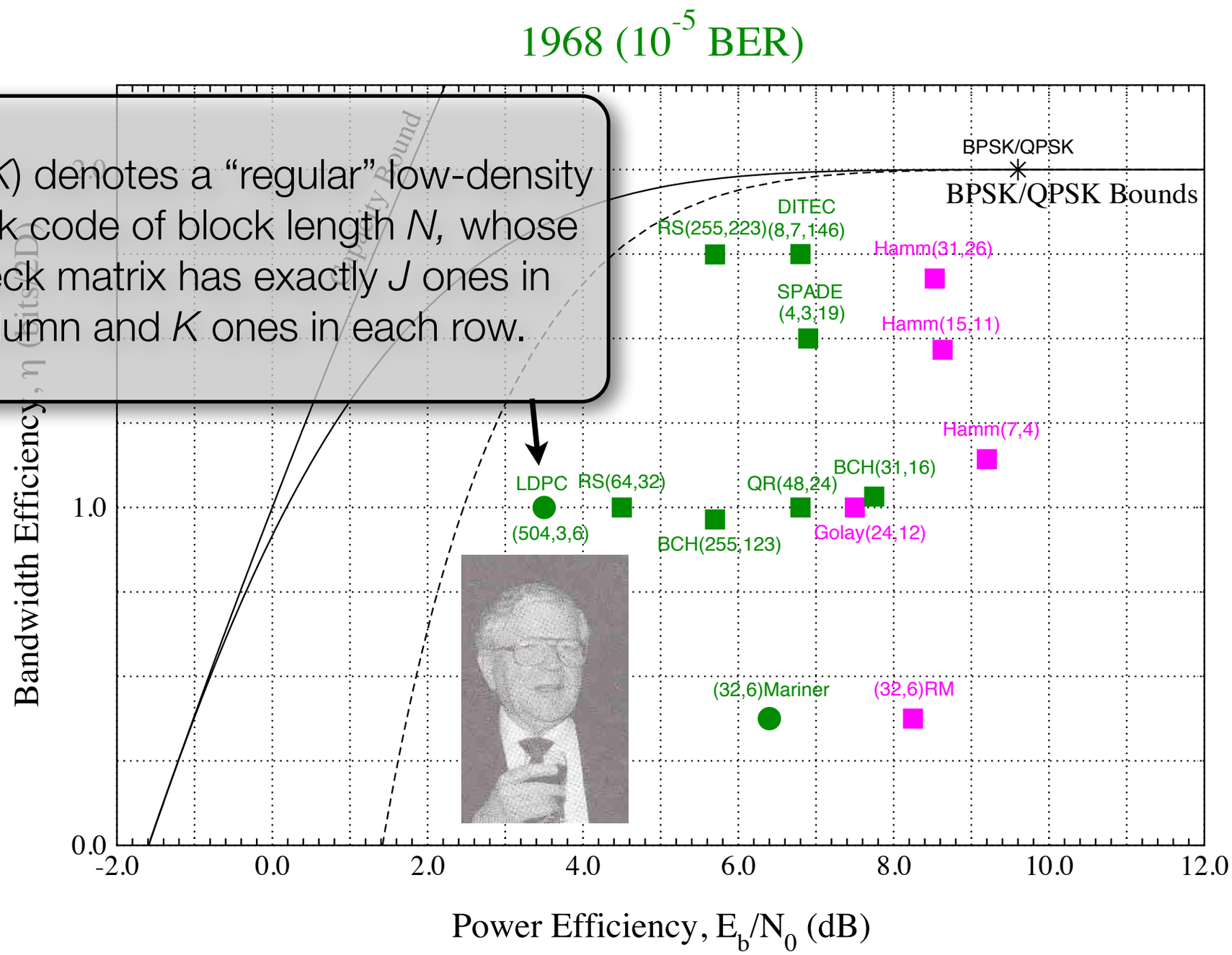
The Second Day



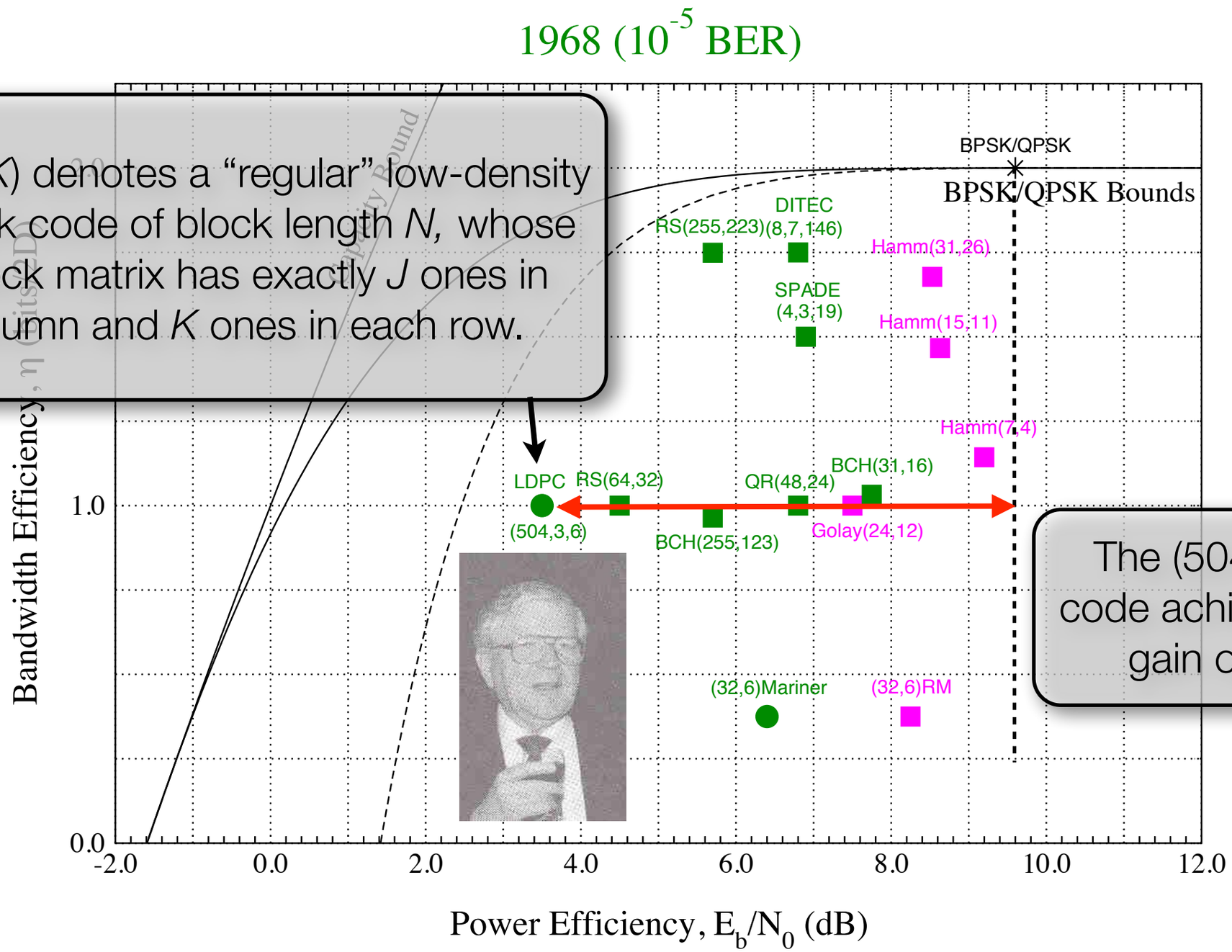
The Second Day



The Second Day



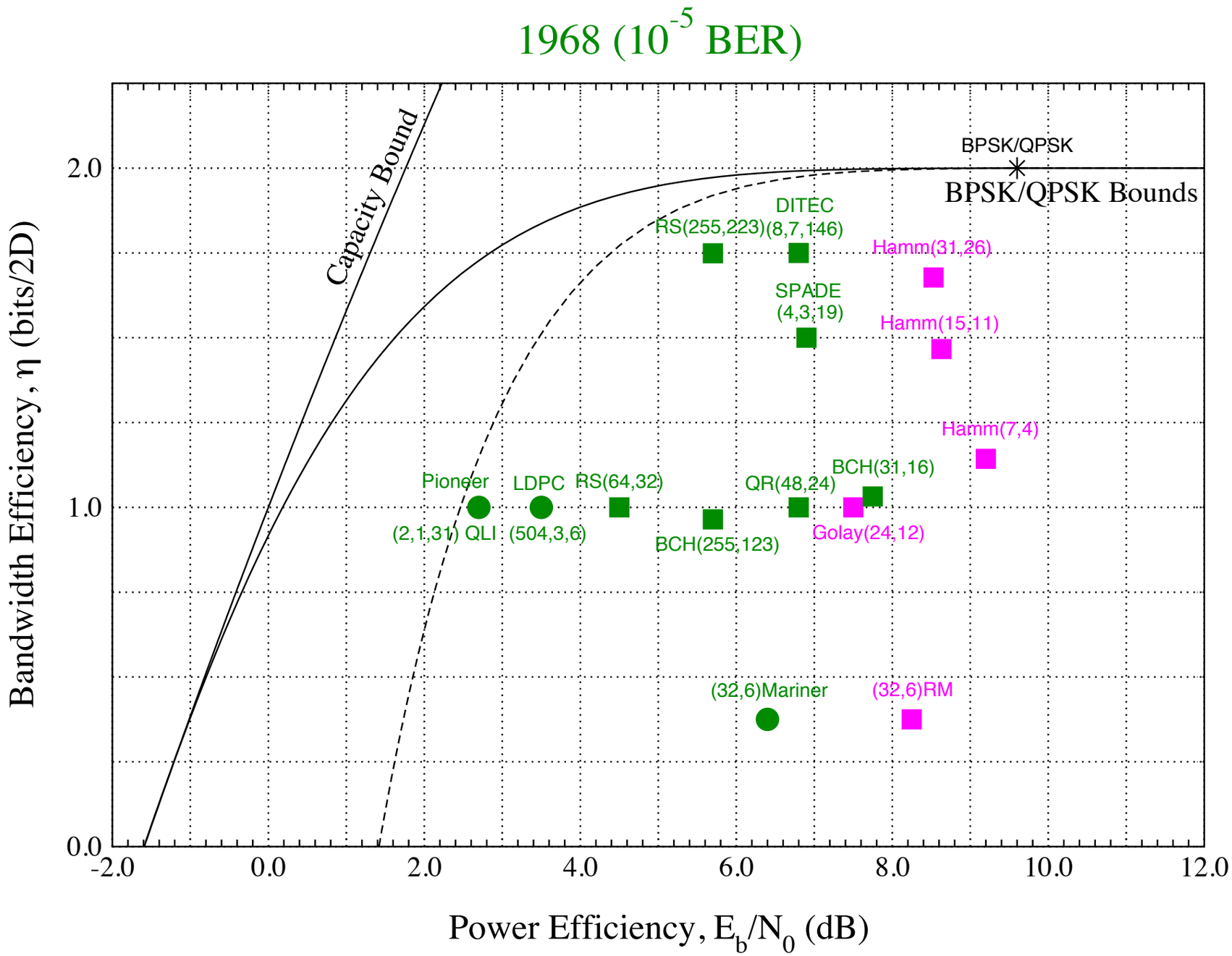
The Second Day



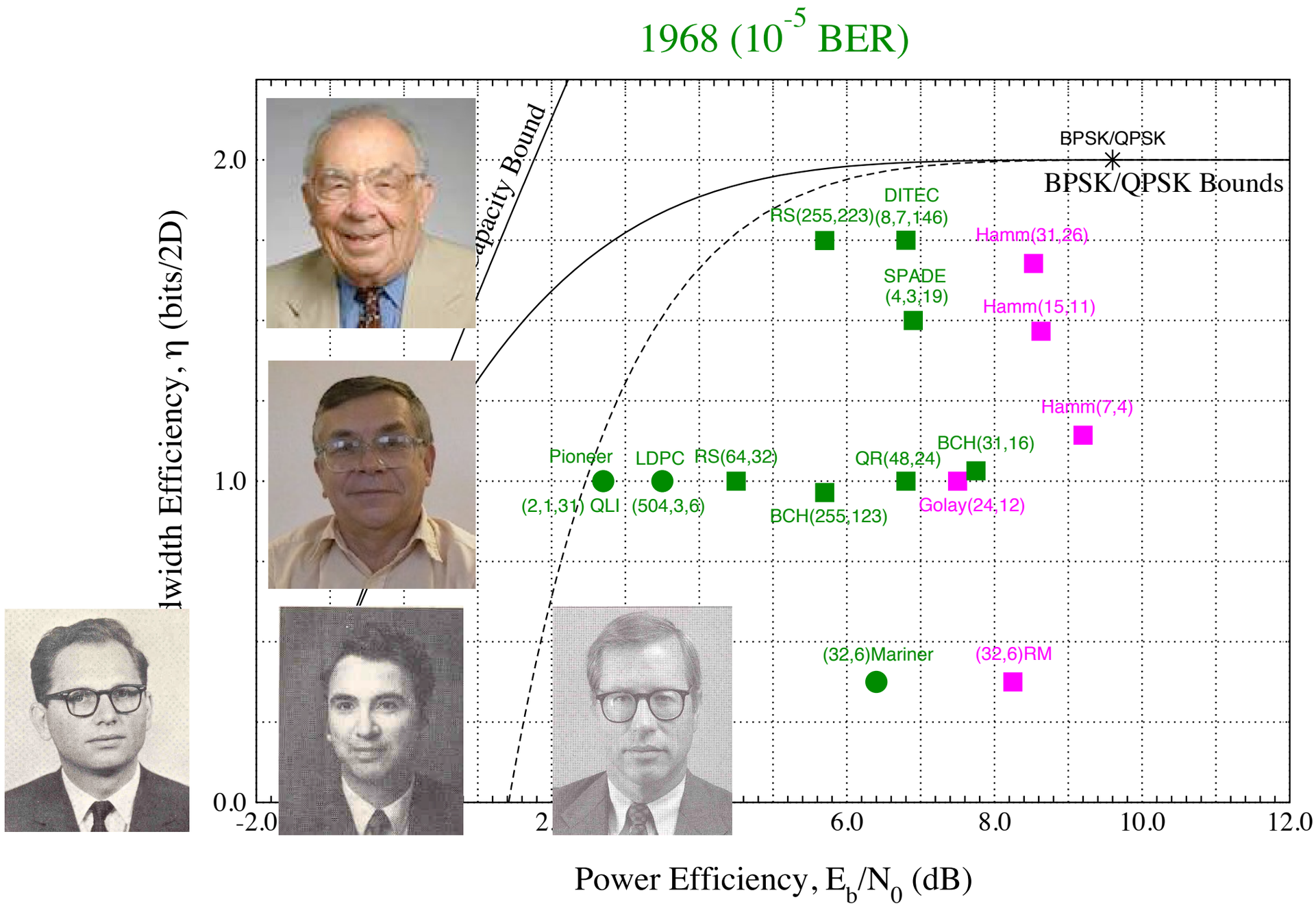
LDPC (*N,J,K*) denotes a "regular" low-density parity-check code of block length *N*, whose parity-check matrix has exactly *J* ones in each column and *K* ones in each row.

The (504,3,6) LDPC code achieves a coding gain of 6.06 dB.

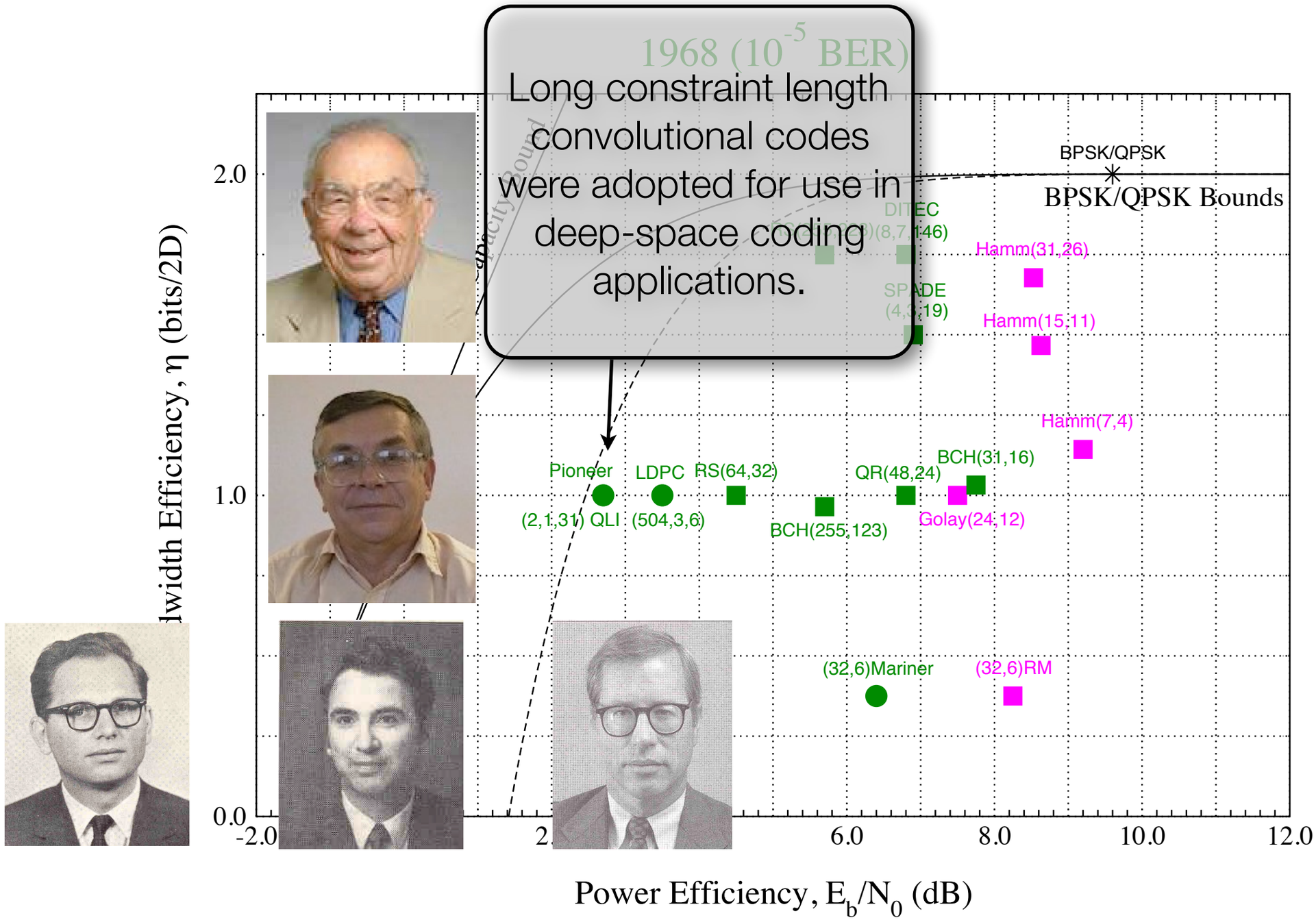
The Second Day



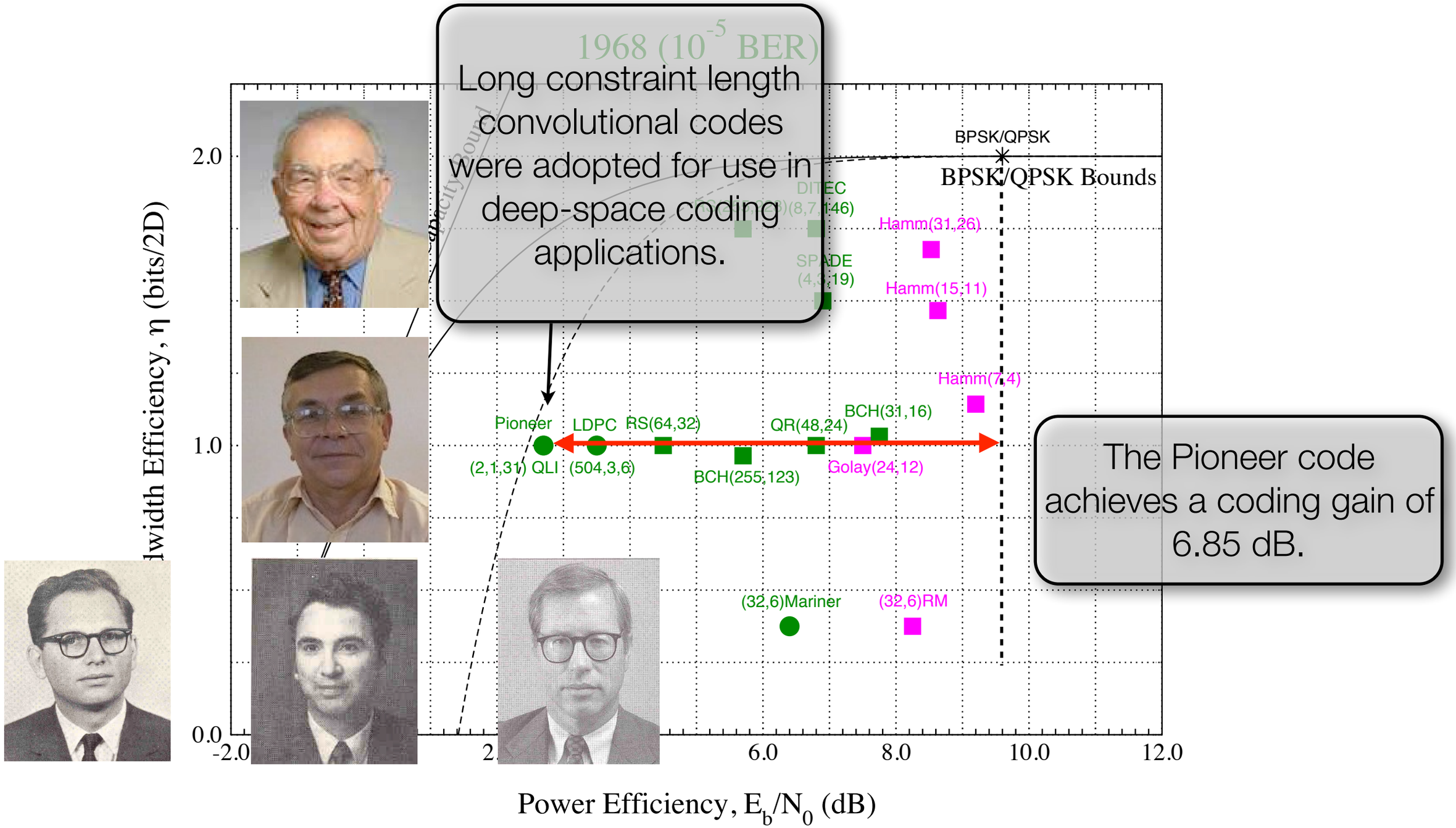
The Second Day



The Second Day



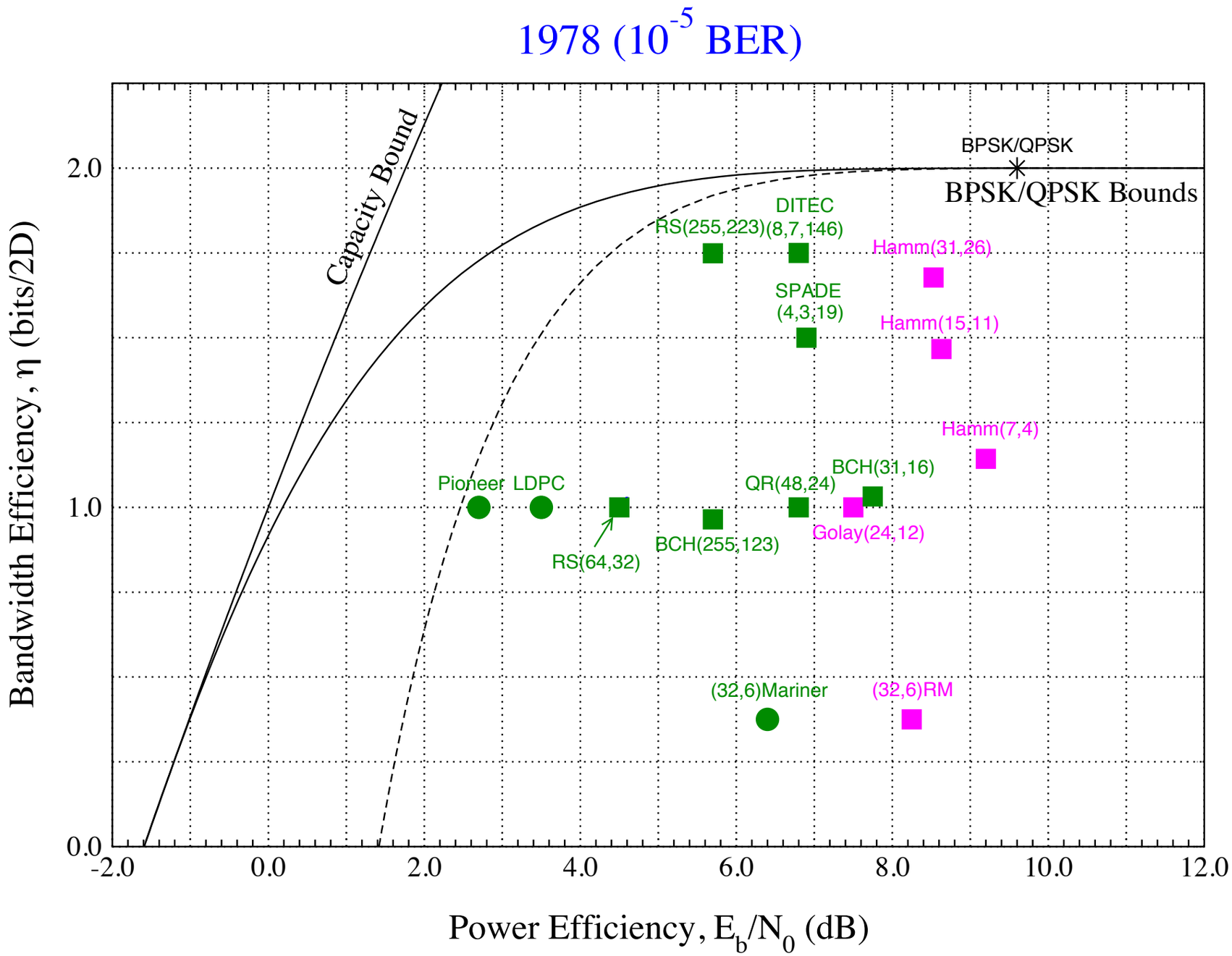
The Second Day



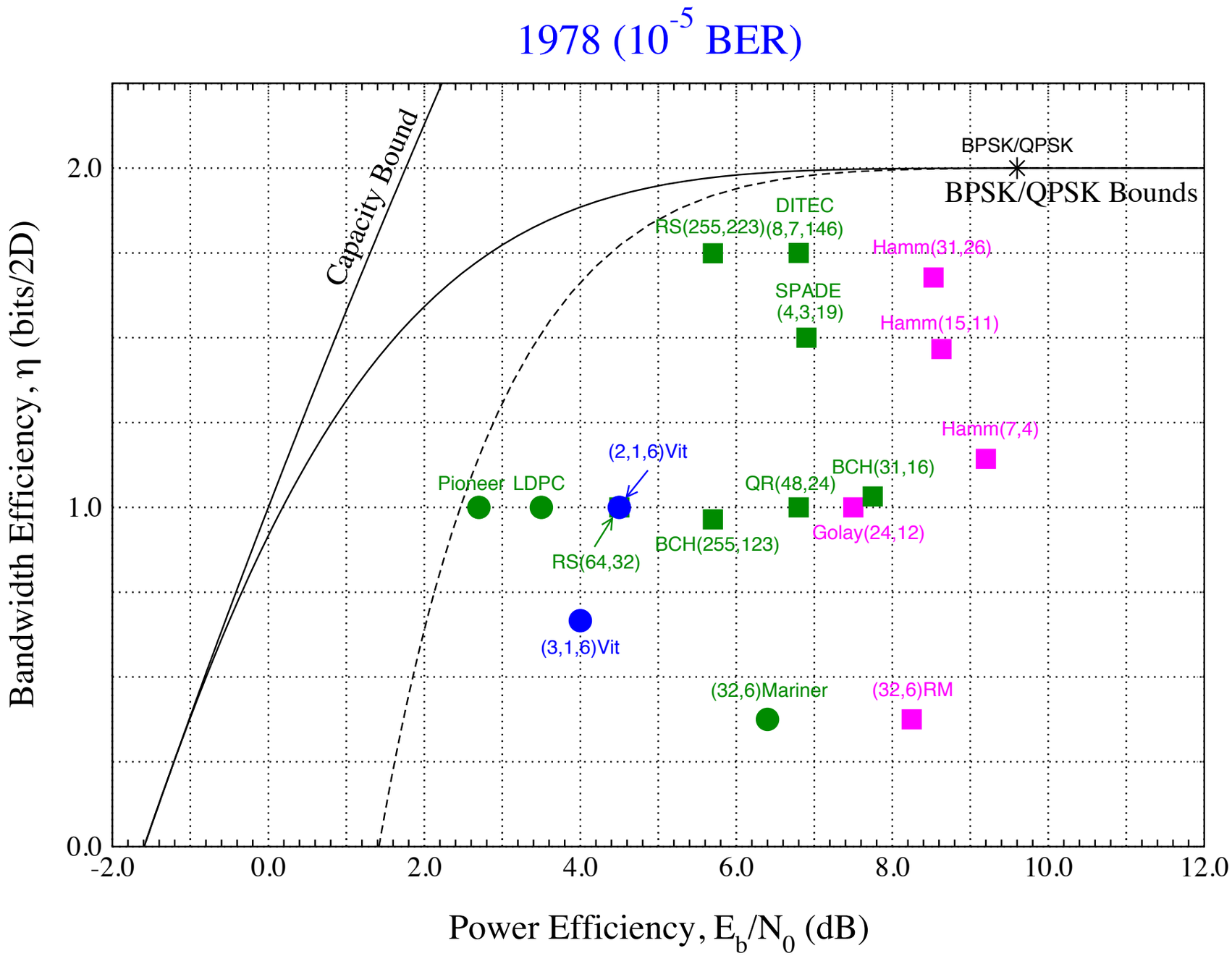
The Third Day

The Third Day

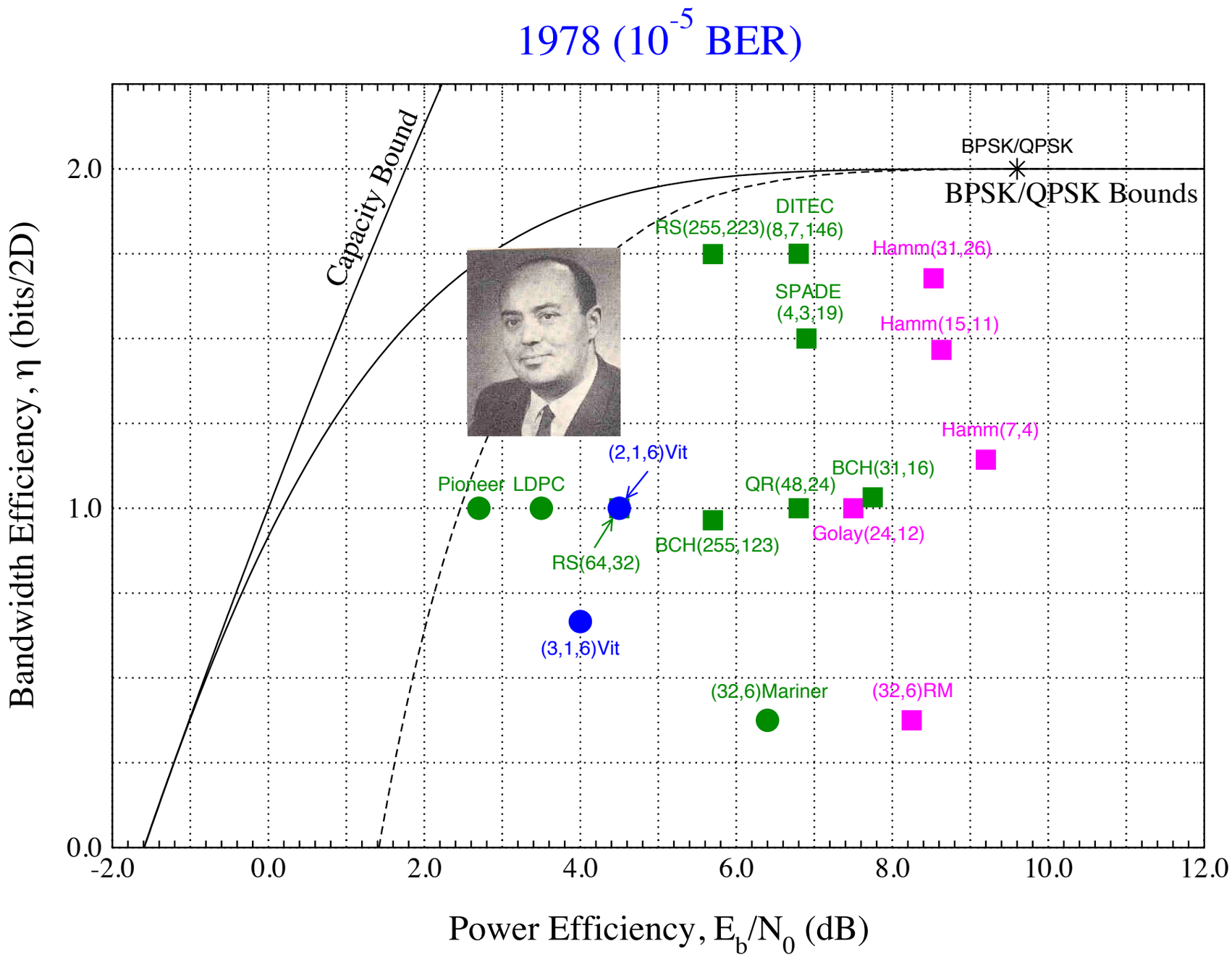
The Third Day



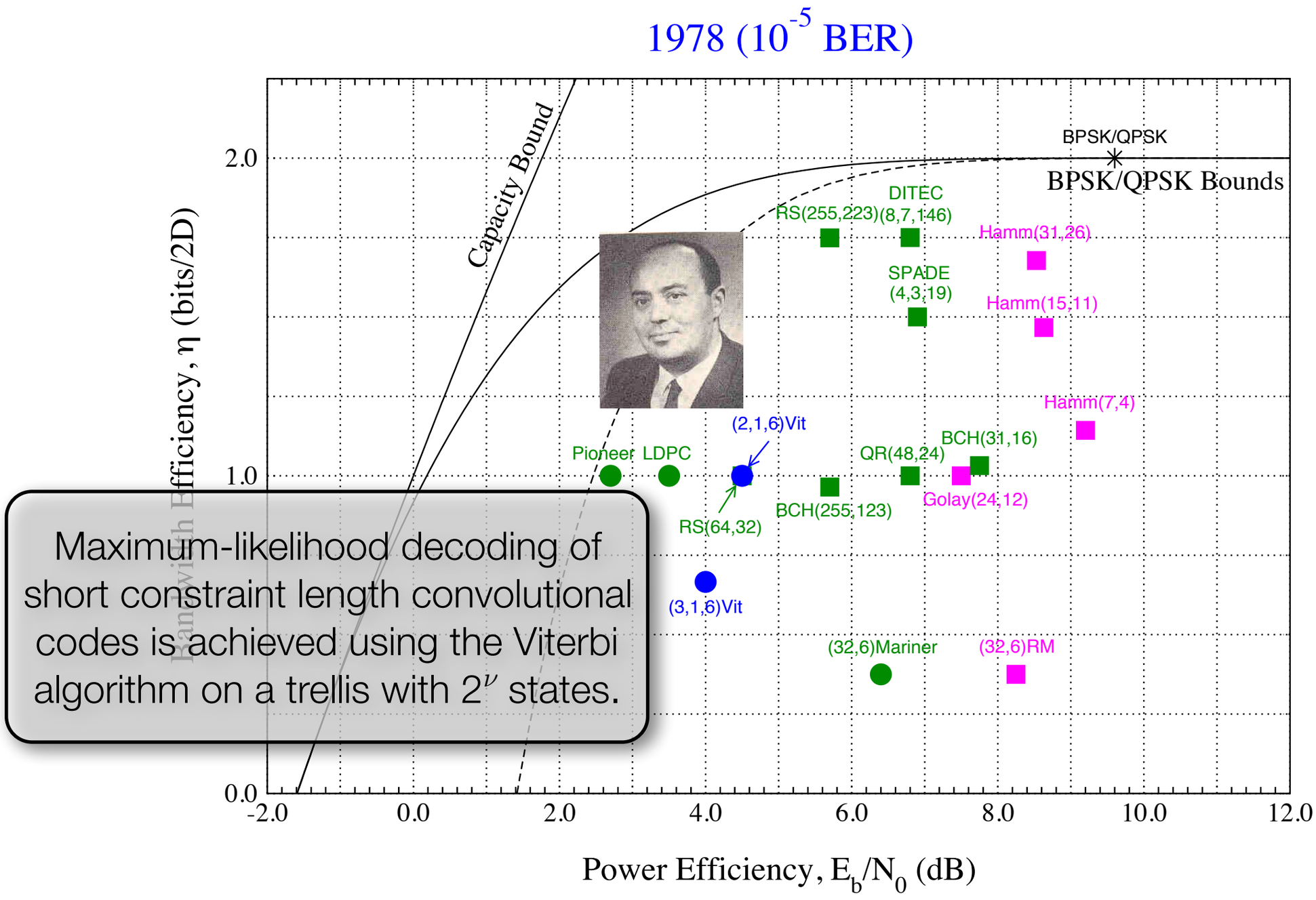
The Third Day



The Third Day

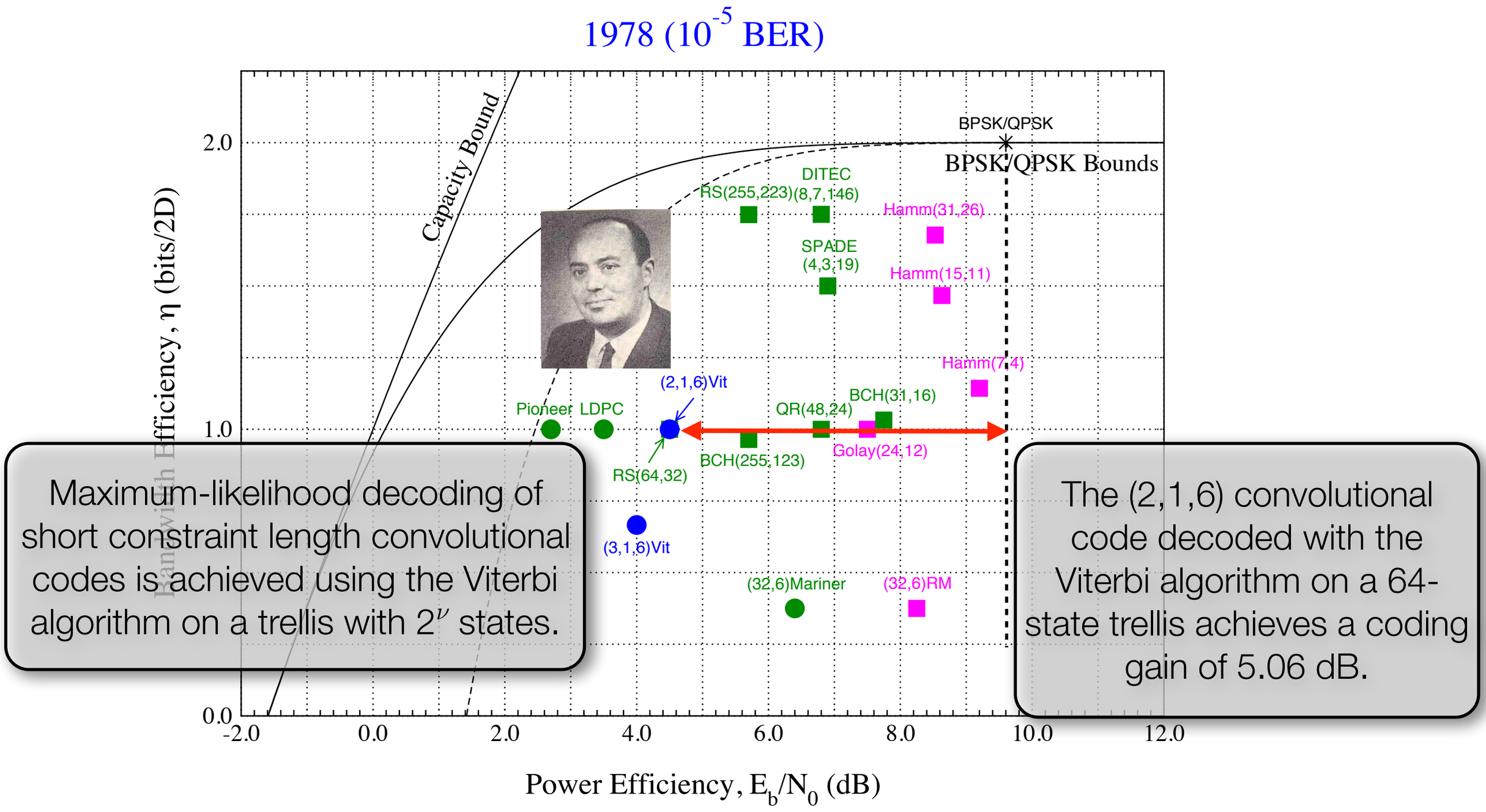


The Third Day



Maximum-likelihood decoding of short constraint length convolutional codes is achieved using the Viterbi algorithm on a trellis with 2^{ν} states.

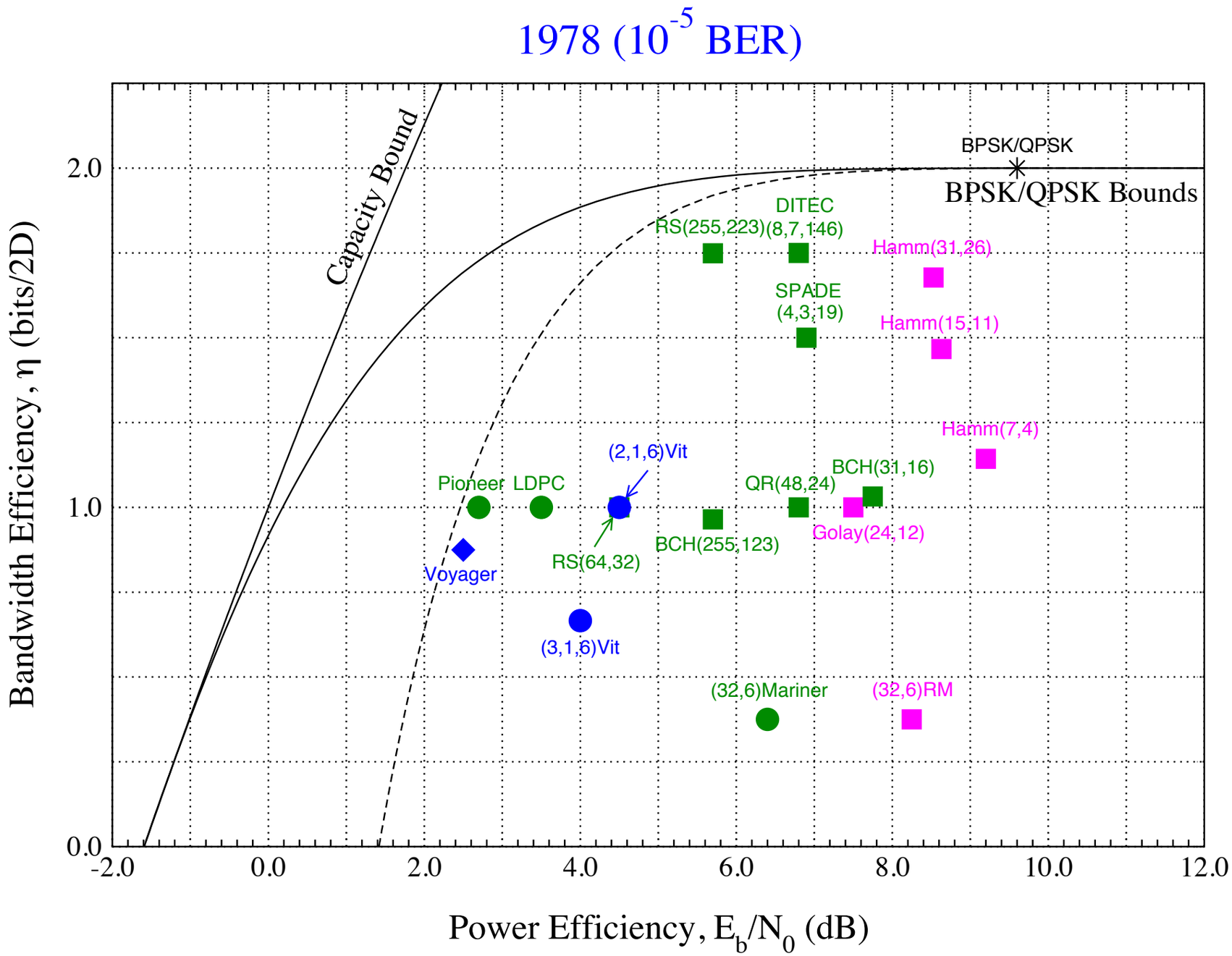
The Third Day



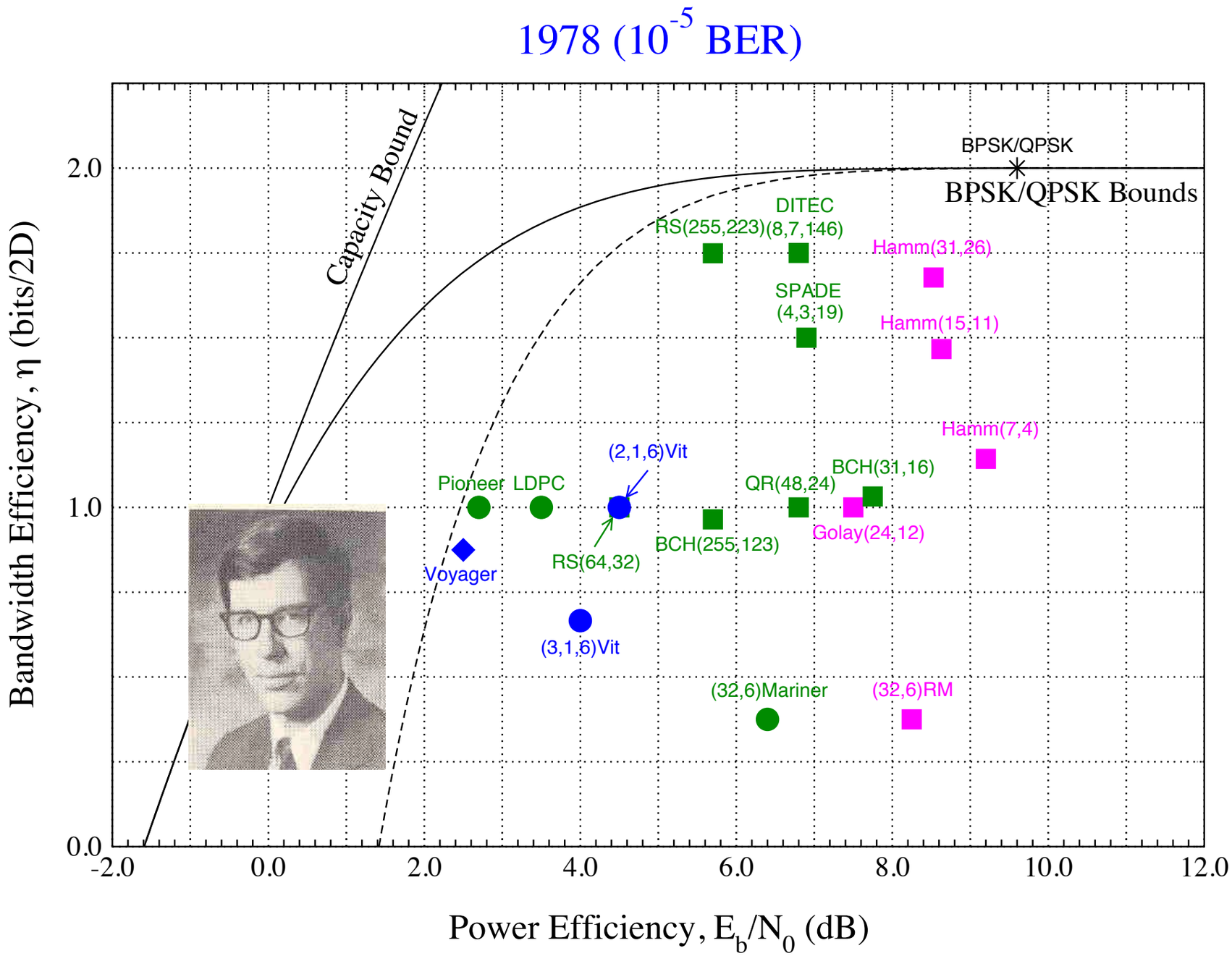
Maximum-likelihood decoding of short constraint length convolutional codes is achieved using the Viterbi algorithm on a trellis with 2^{ν} states.

The (2,1,6) convolutional code decoded with the Viterbi algorithm on a 64-state trellis achieves a coding gain of 5.06 dB.

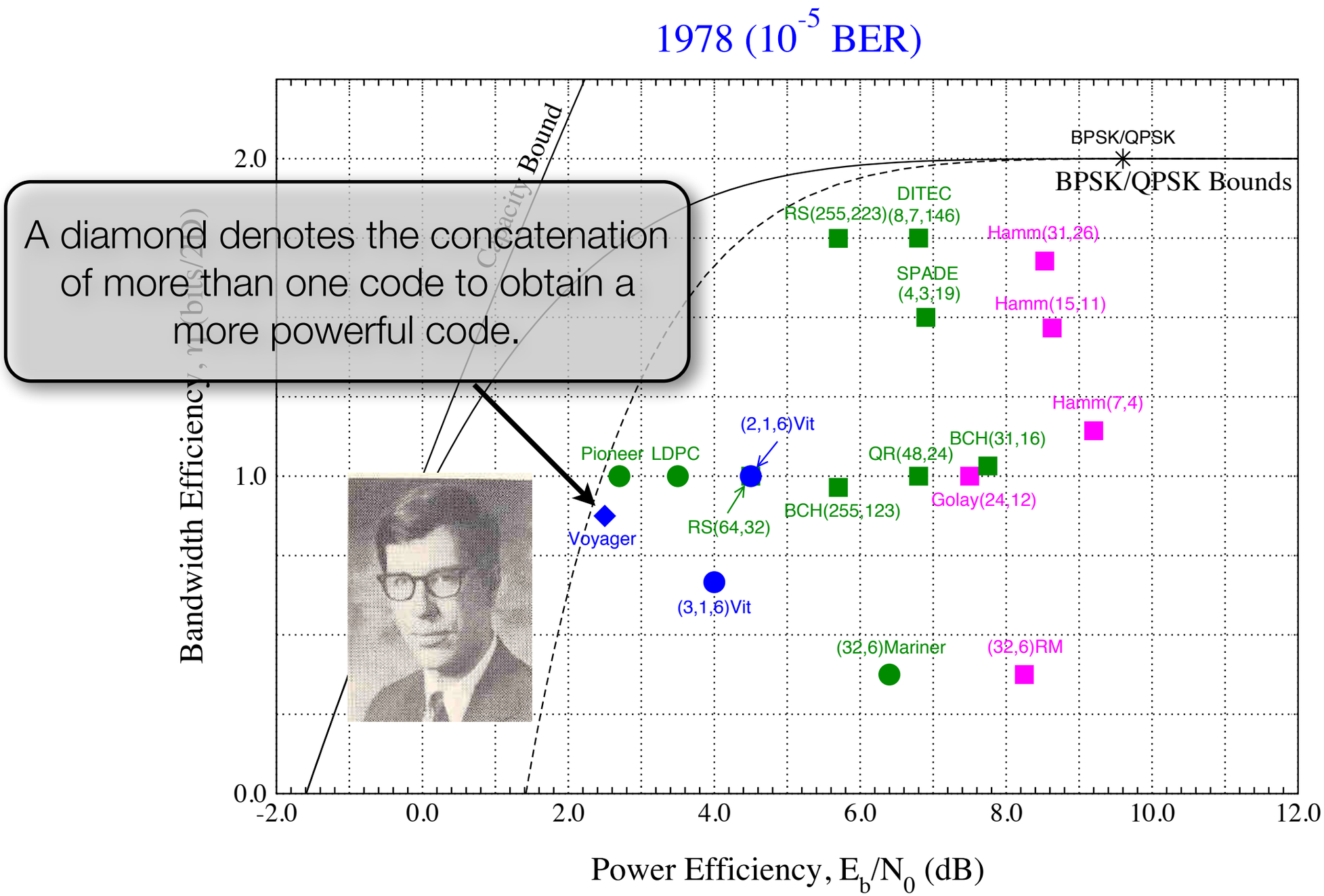
The Third Day



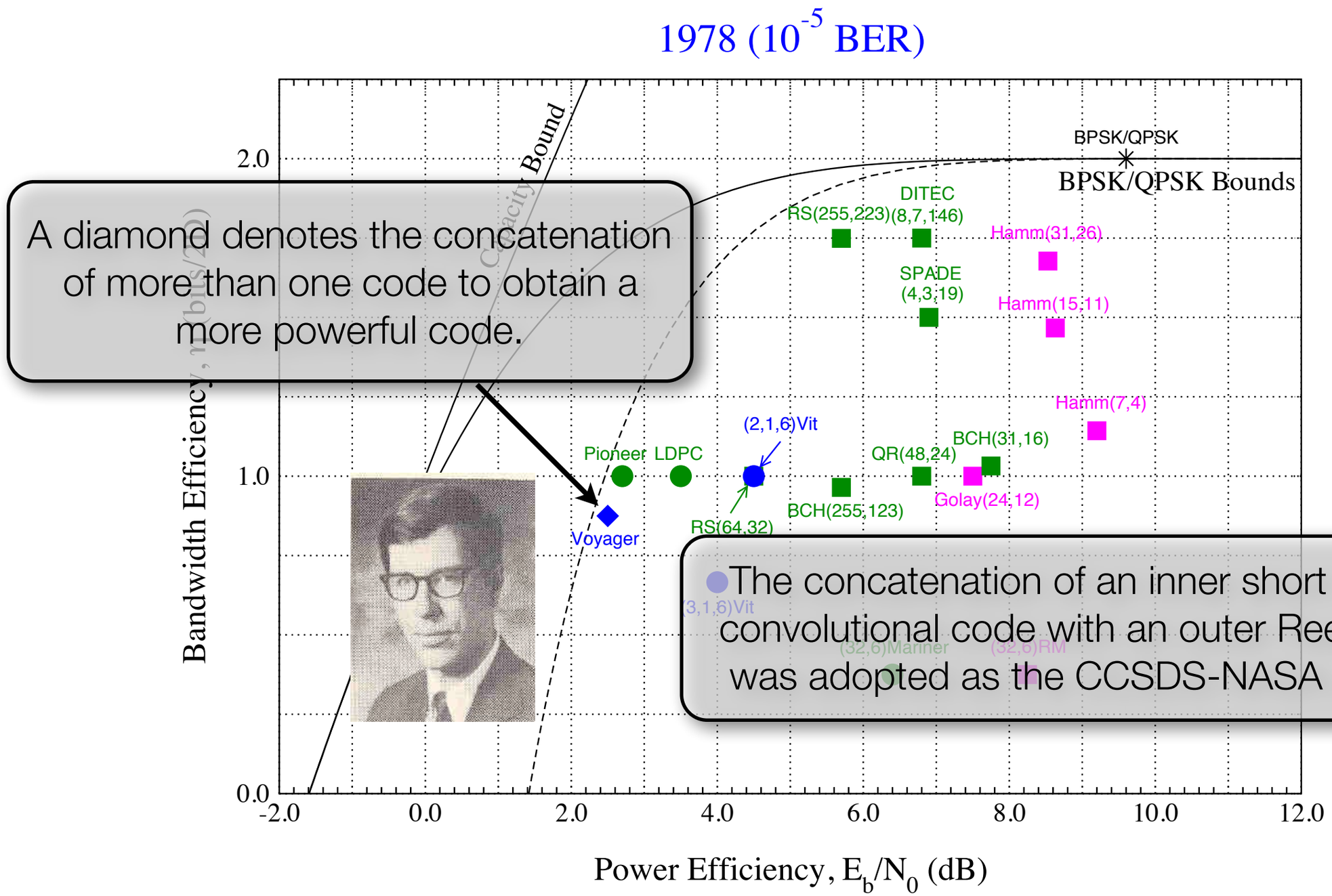
The Third Day



The Third Day



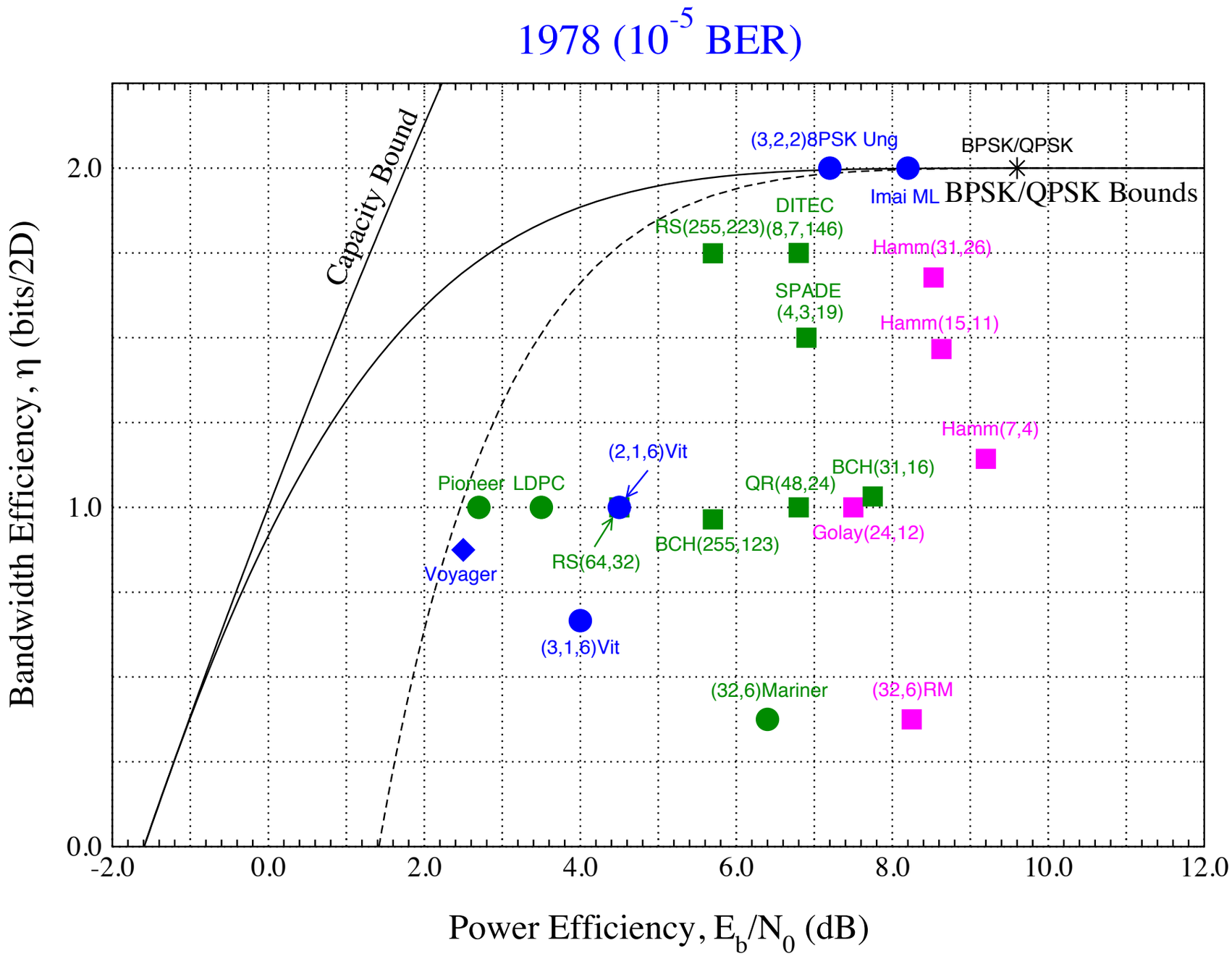
The Third Day



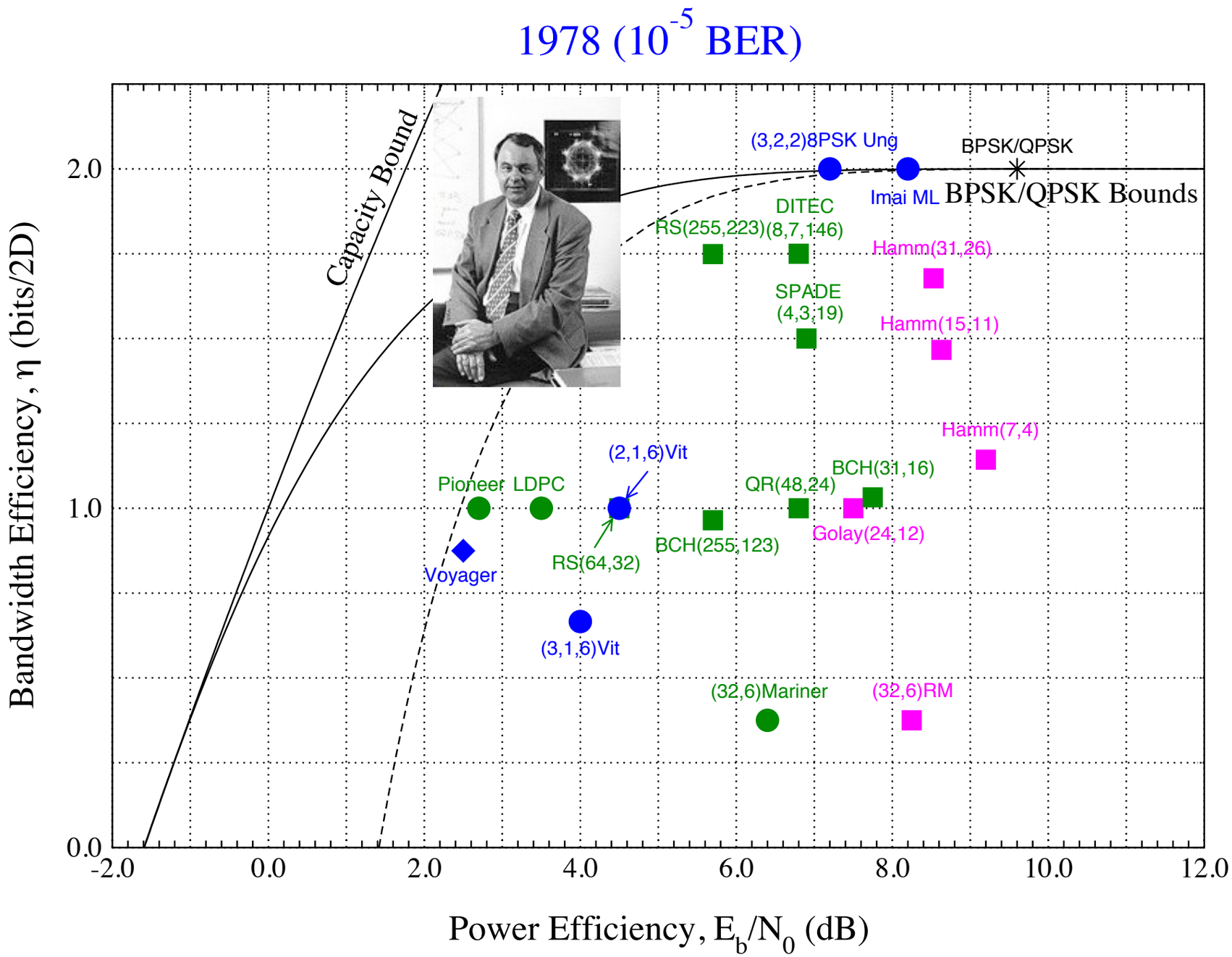
A diamond denotes the concatenation of more than one code to obtain a more powerful code.

The concatenation of an inner short constraint length convolutional code with an outer Reed-Solomon code was adopted as the CCSDS-NASA coding standard.

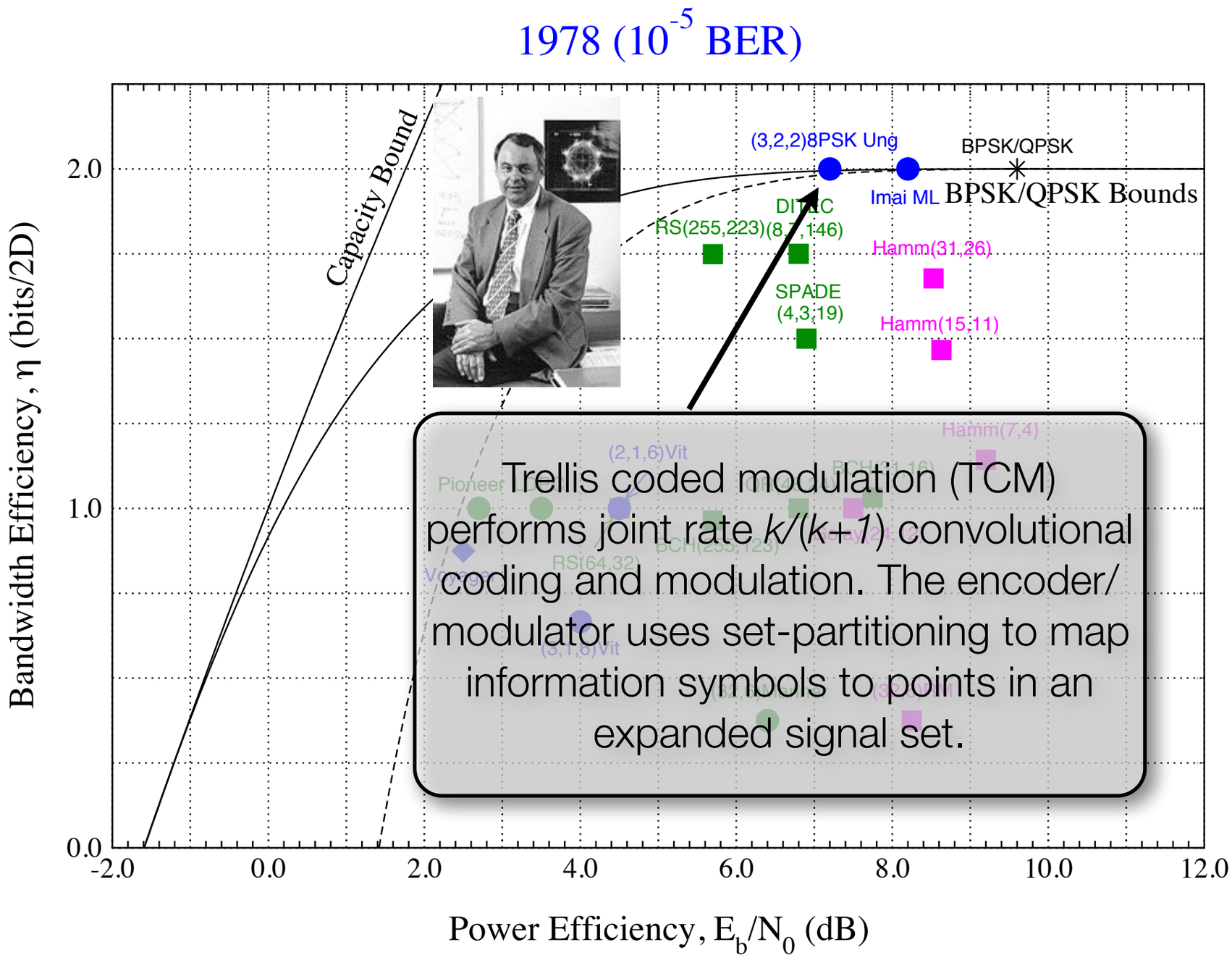
The Third Day



The Third Day

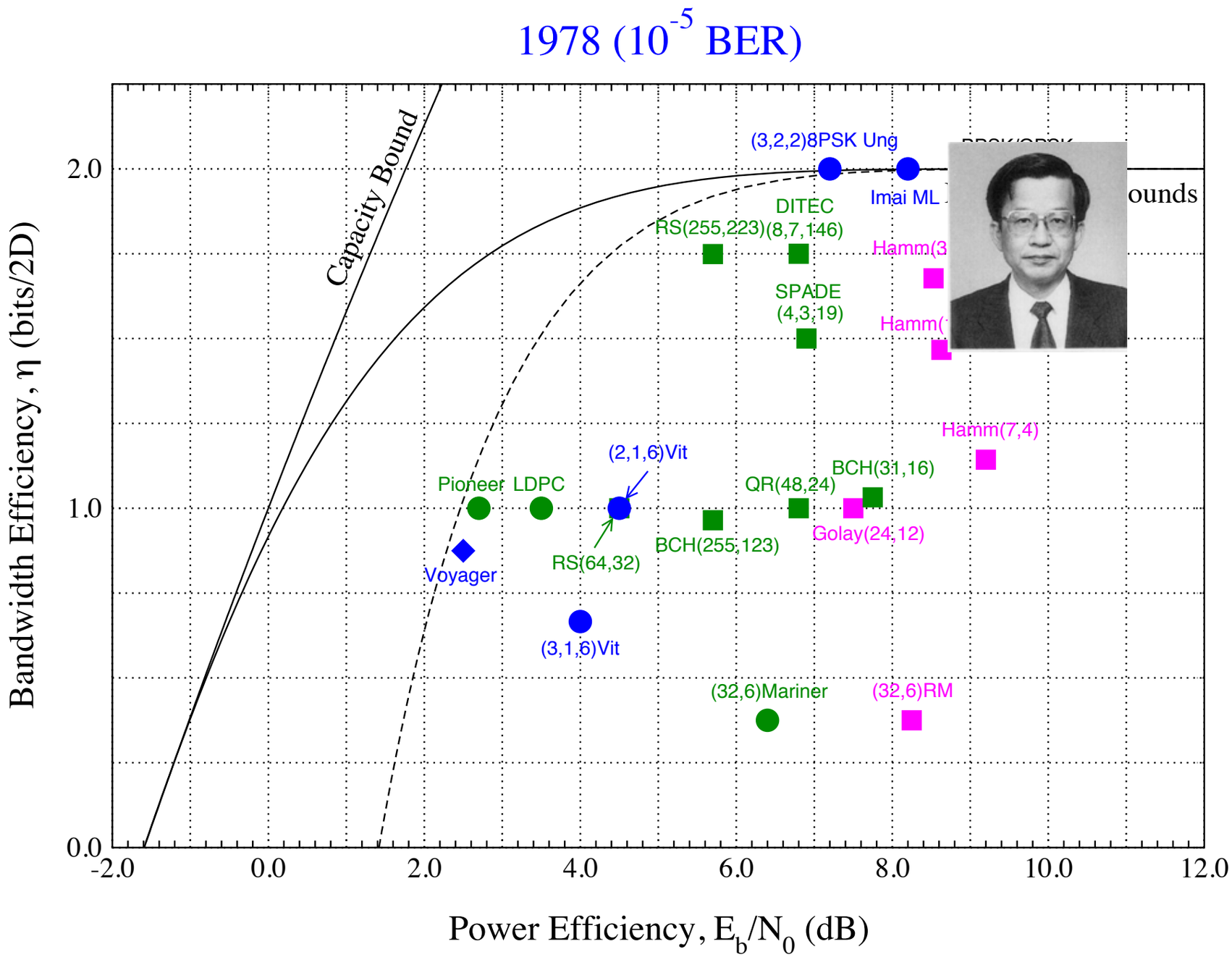


The Third Day

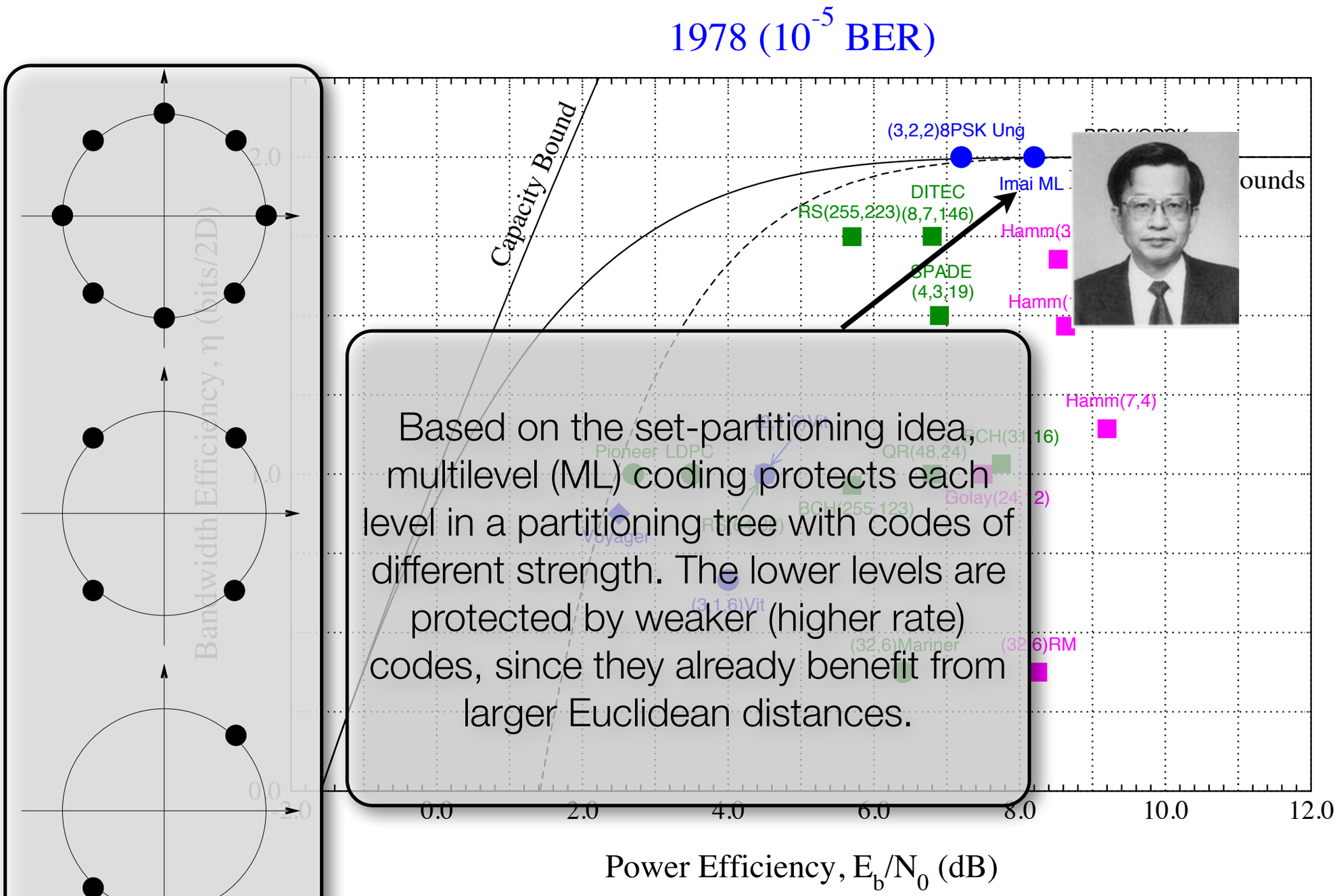


Trellis coded modulation (TCM) performs joint rate *k/(k+1)* convolutional coding and modulation. The encoder/modulator uses set-partitioning to map information symbols to points in an expanded signal set.

The Third Day

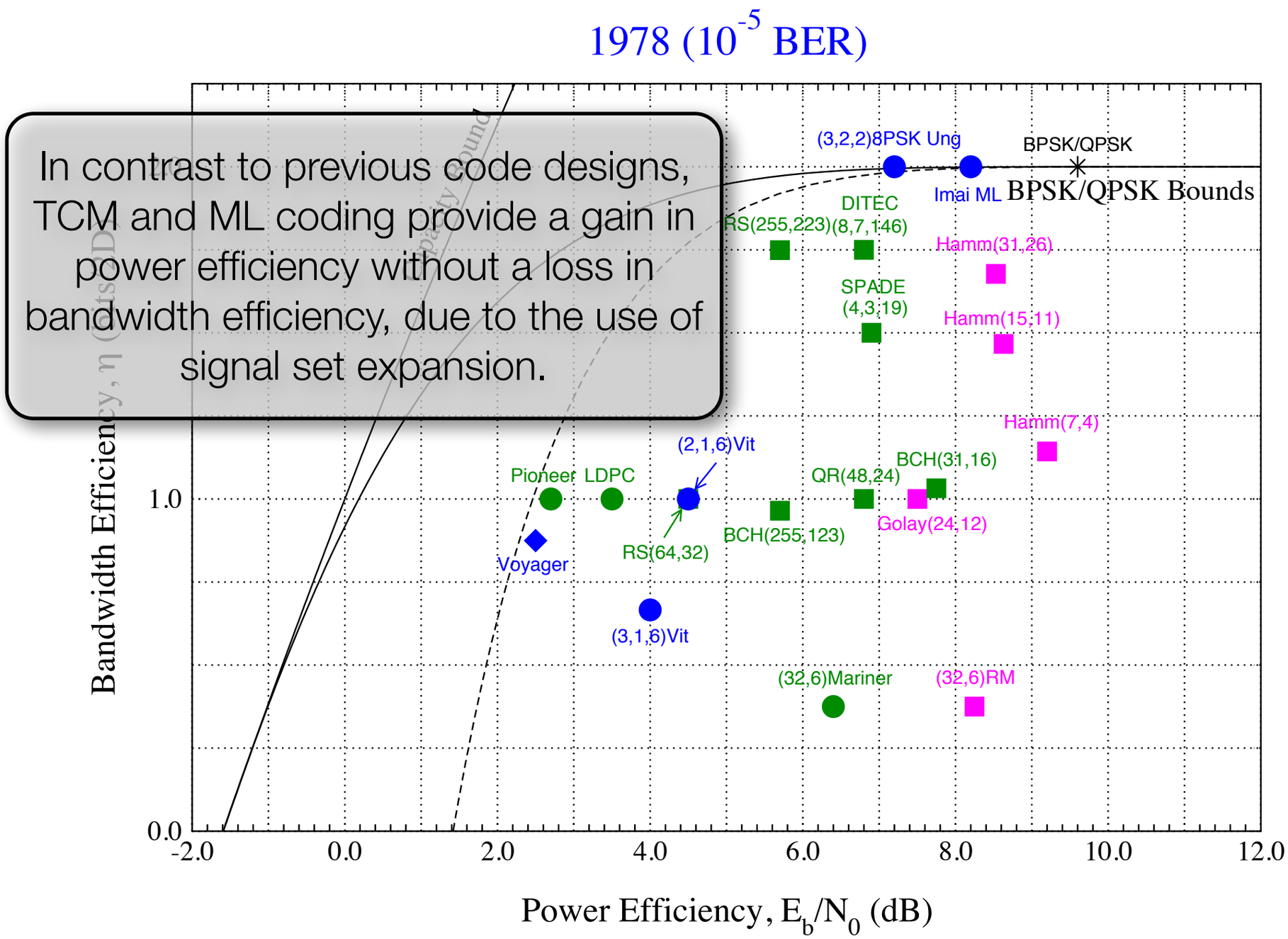


The Third Day



Based on the set-partitioning idea, multilevel (ML) coding protects each level in a partitioning tree with codes of different strength. The lower levels are protected by weaker (higher rate) codes, since they already benefit from larger Euclidean distances.

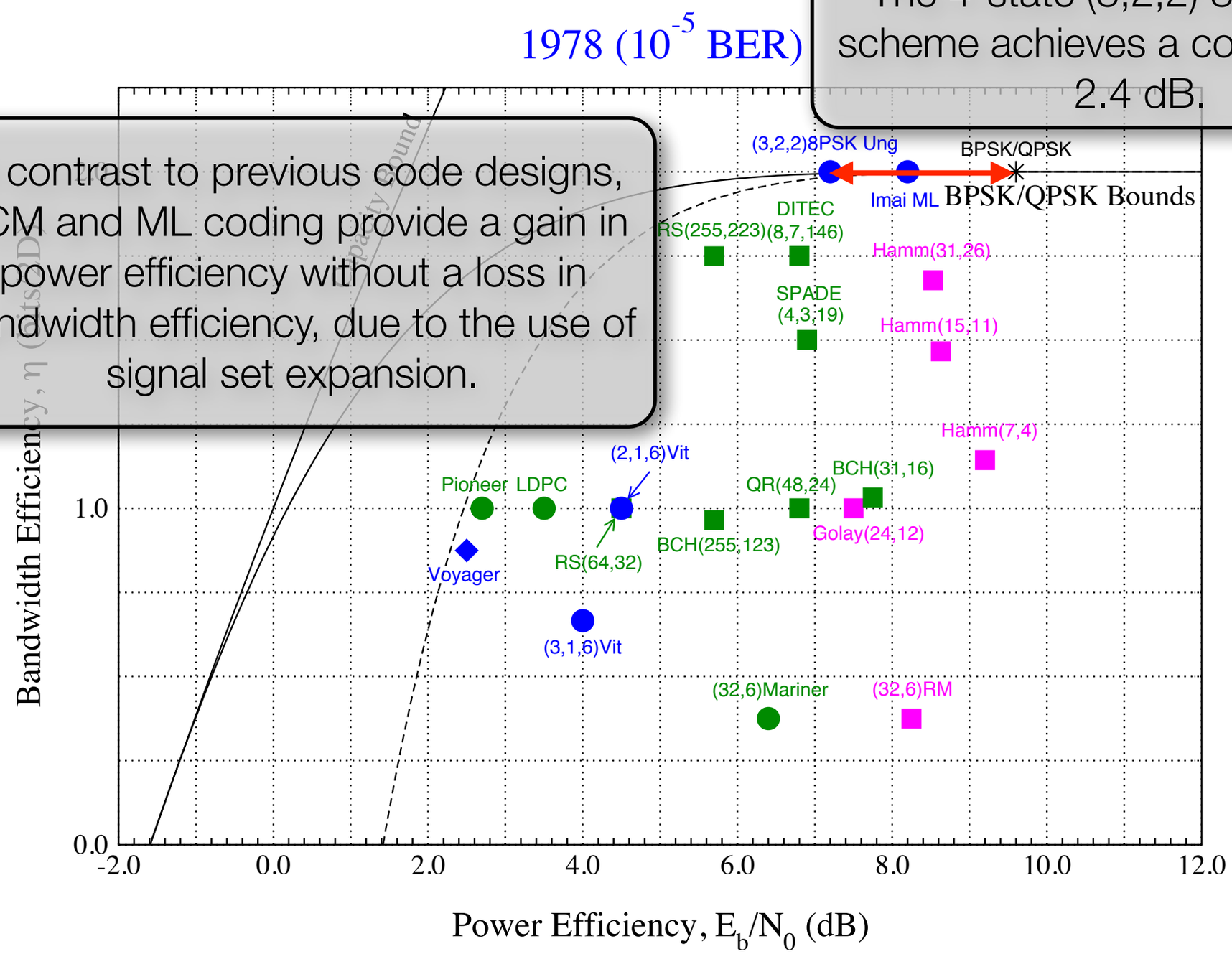
The Third Day



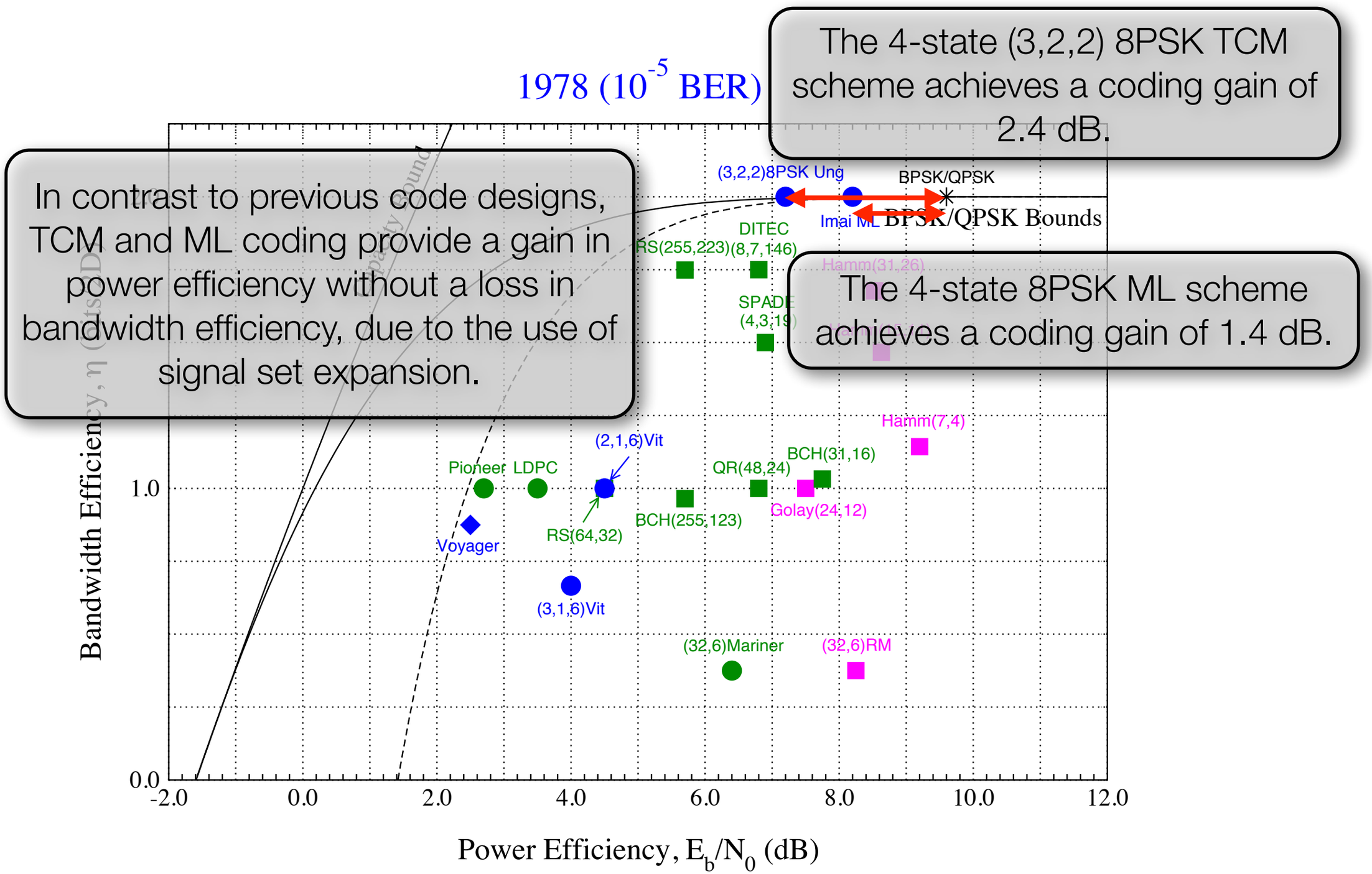
The Third Day

The 4-state (3,2,2) 8PSK TCM scheme achieves a coding gain of 2.4 dB.

In contrast to previous code designs, TCM and ML coding provide a gain in power efficiency without a loss in bandwidth efficiency, due to the use of signal set expansion.



The Third Day



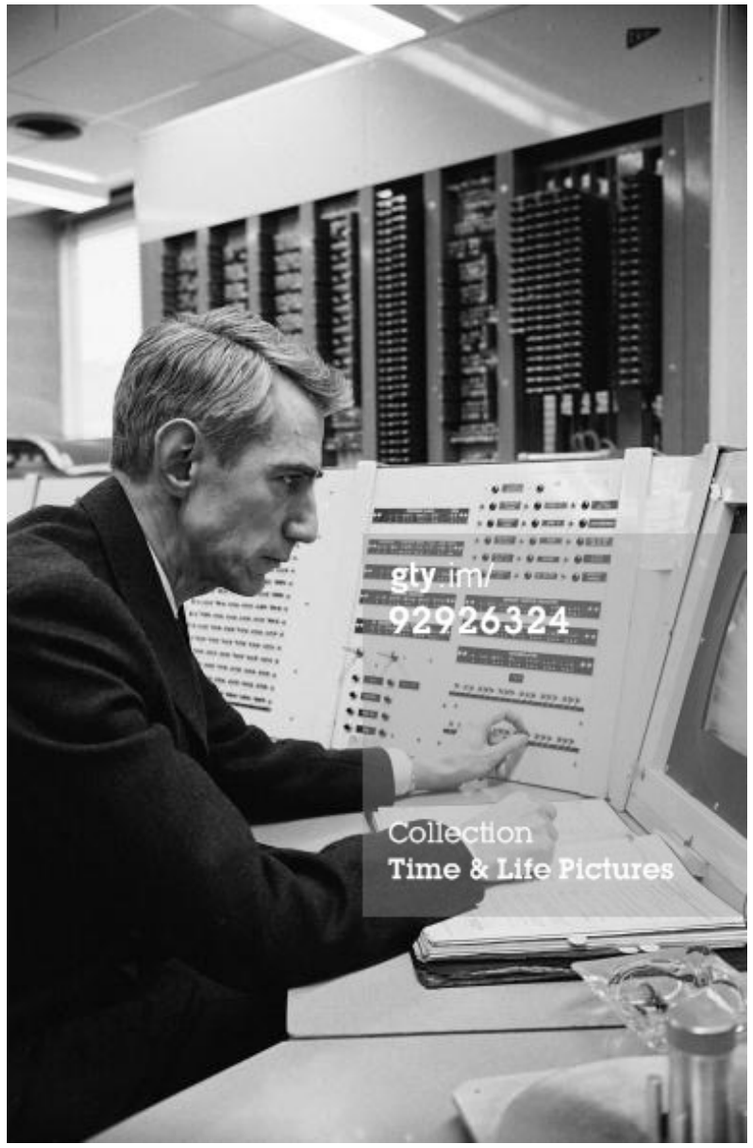
The 4-state (3,2,2) 8PSK TCM scheme achieves a coding gain of 2.4 dB.

In contrast to previous code designs, TCM and ML coding provide a gain in power efficiency without a loss in bandwidth efficiency, due to the use of signal set expansion.

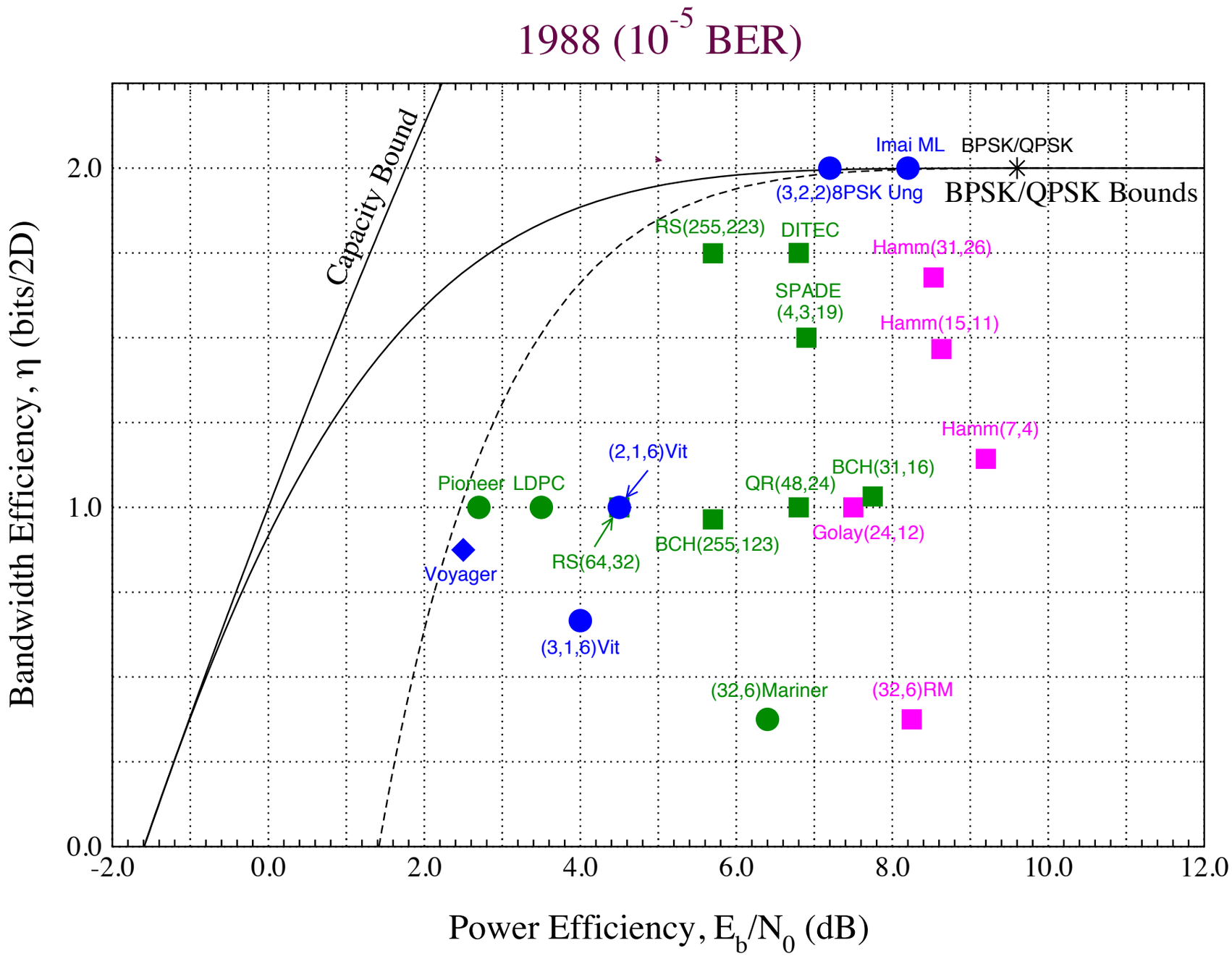
The 4-state 8PSK ML scheme achieves a coding gain of 1.4 dB.

The Fourth Day

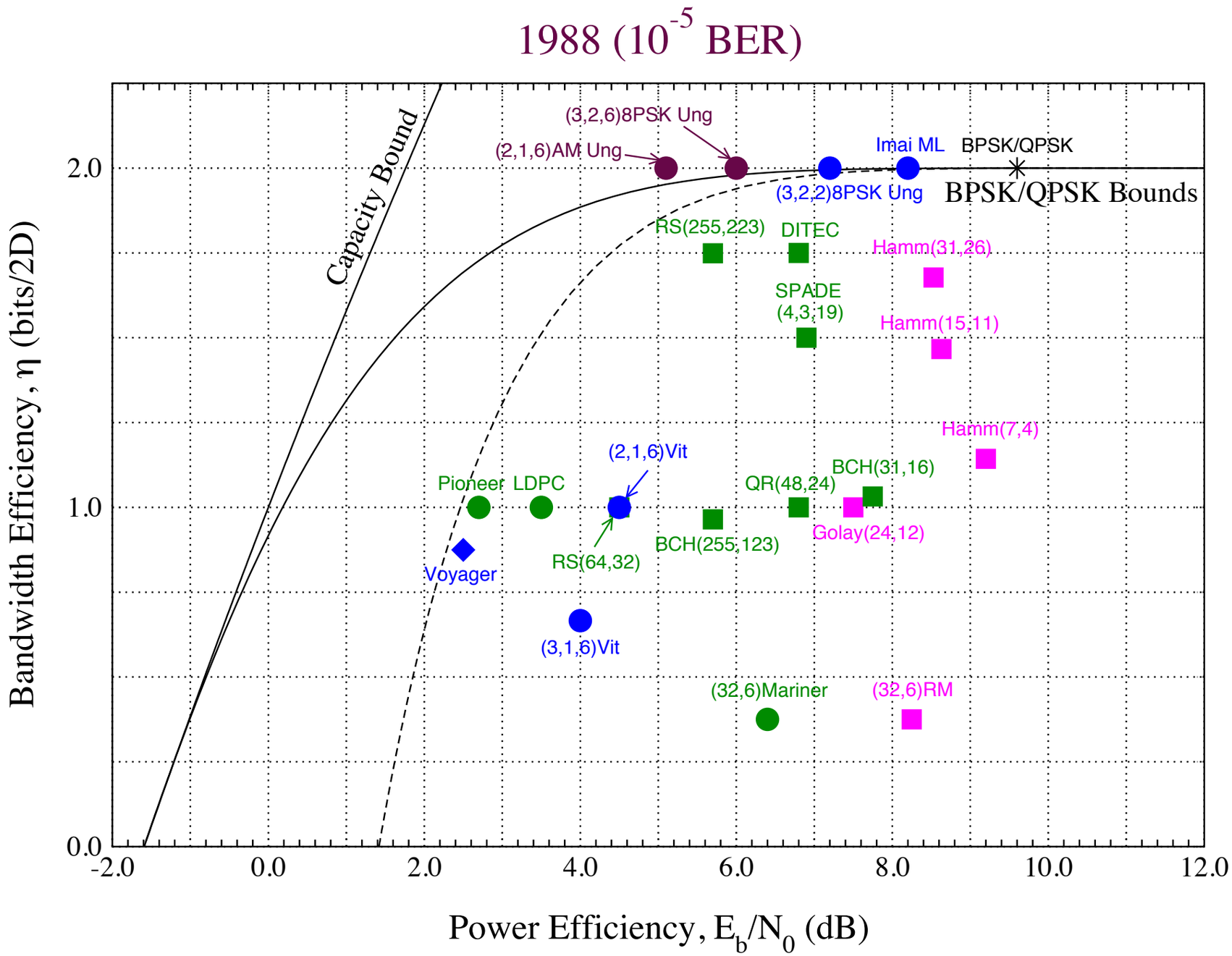
The Fourth Day



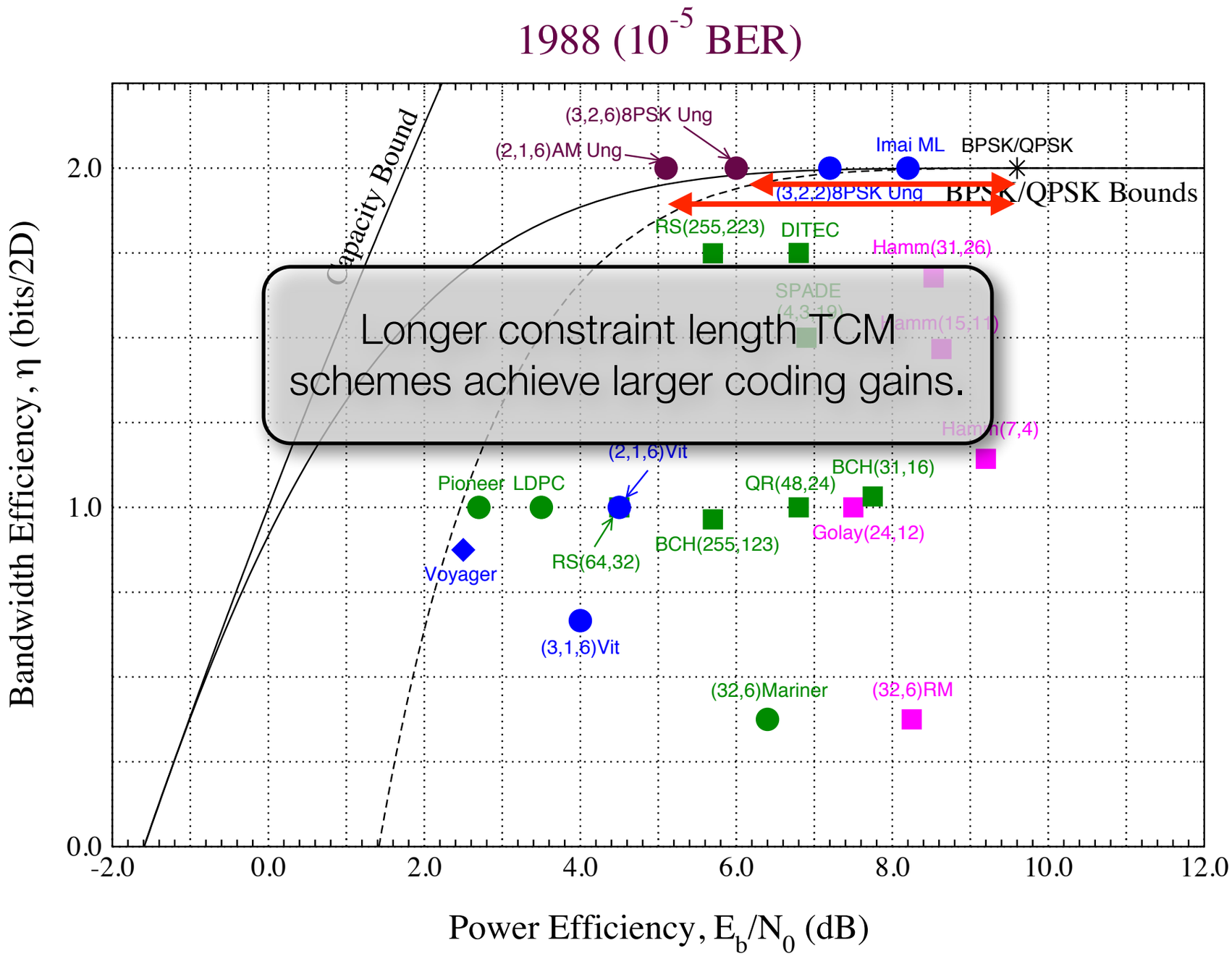
The Fourth Day



The Fourth Day

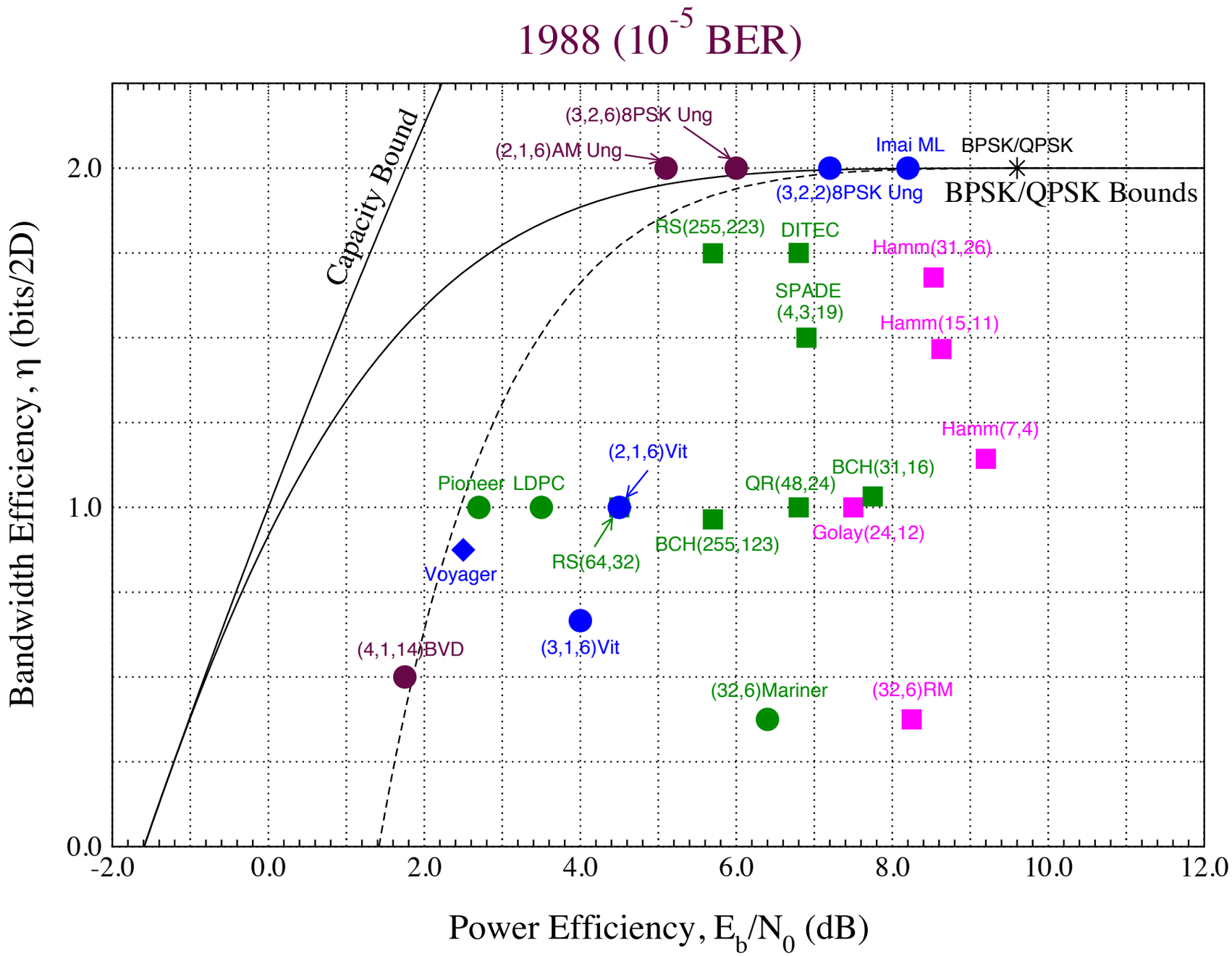


The Fourth Day

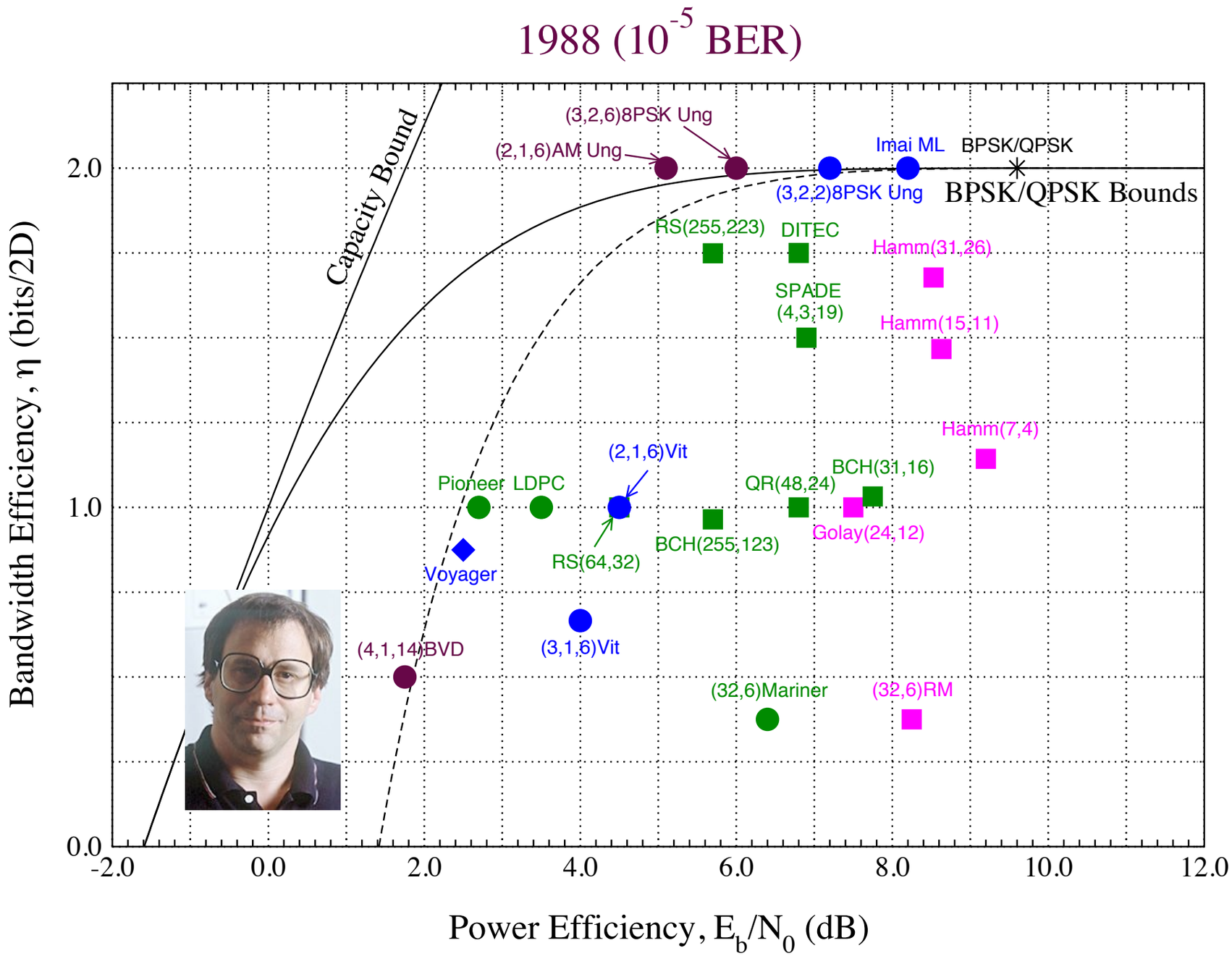


Longer constraint length TCM schemes achieve larger coding gains.

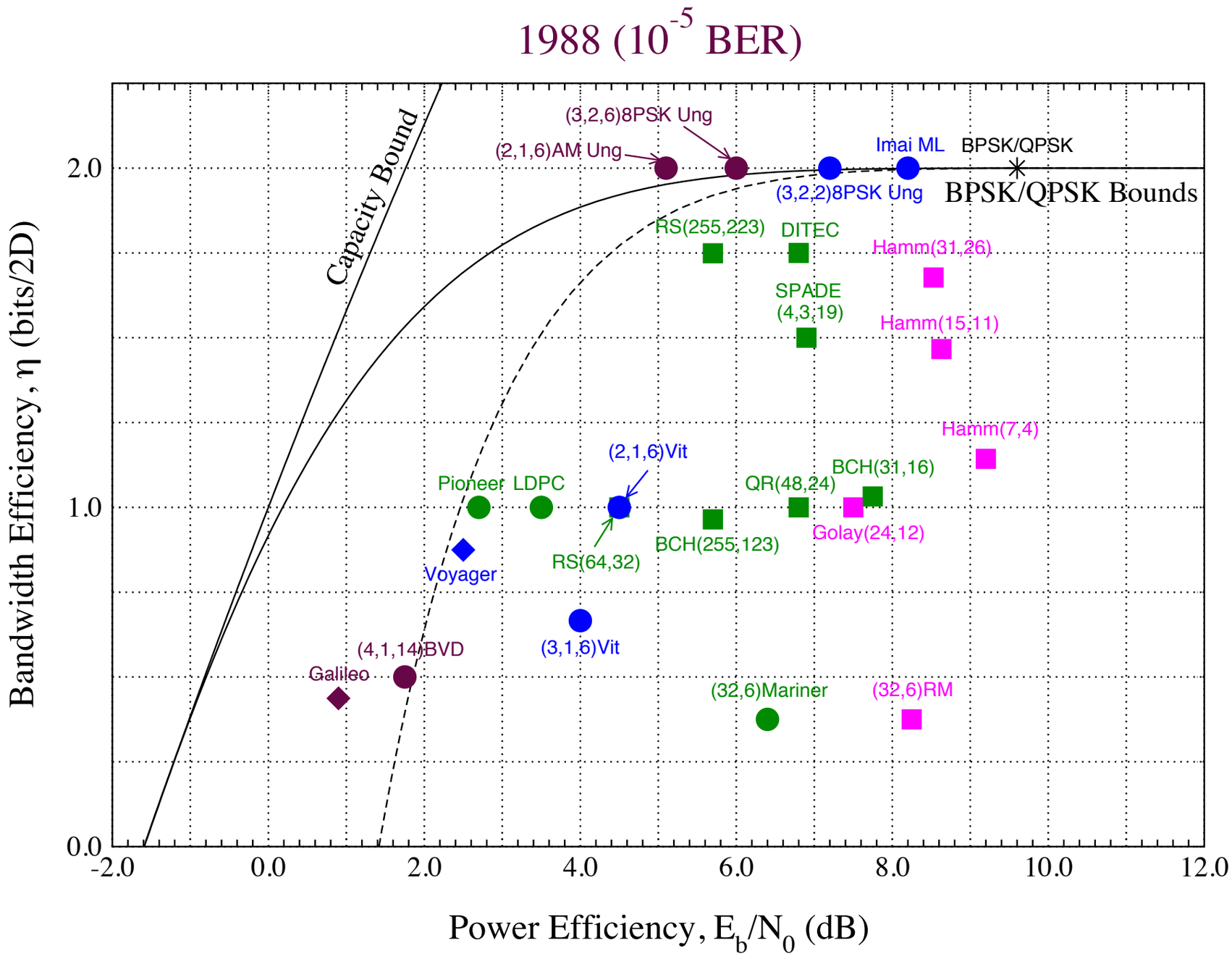
The Fourth Day



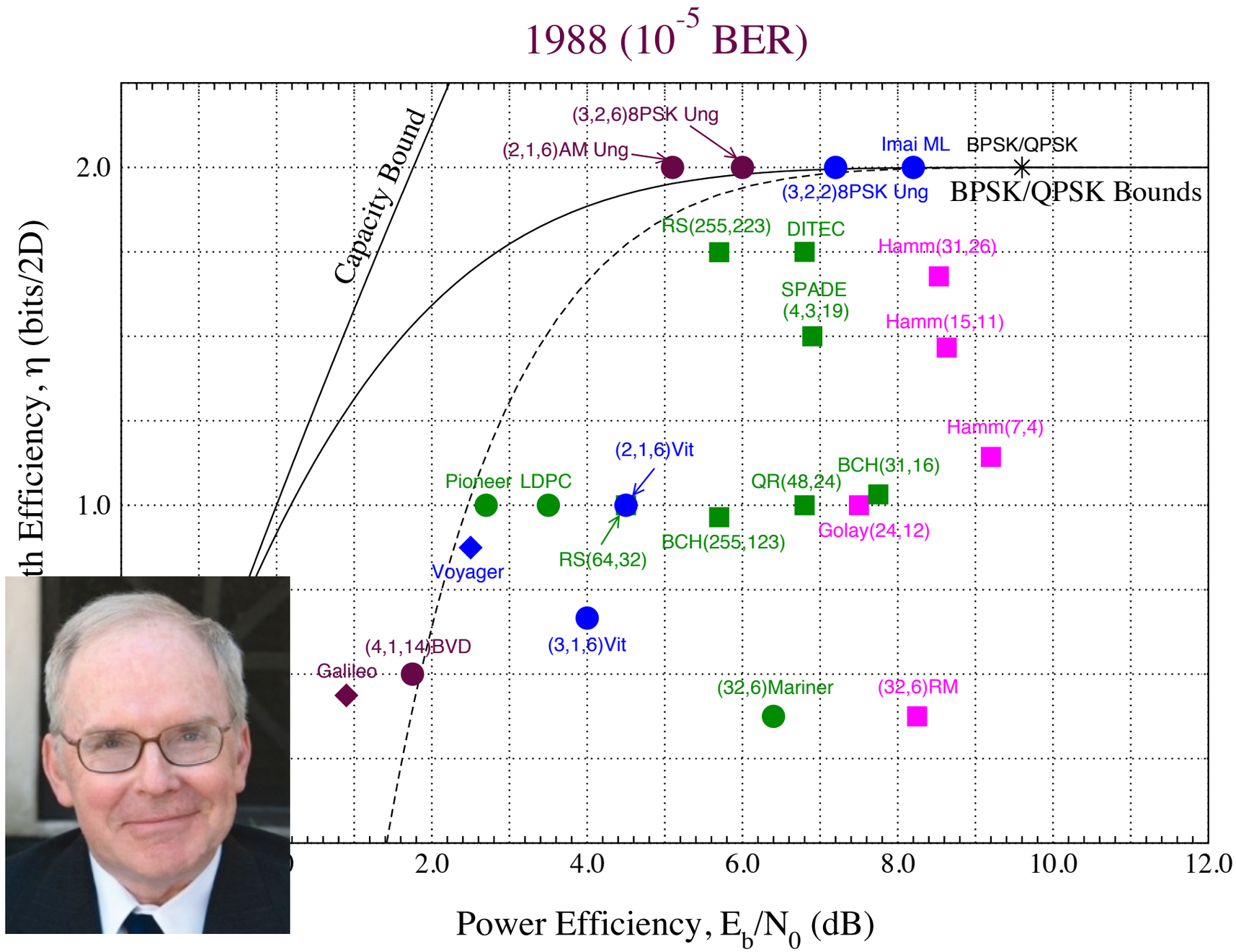
The Fourth Day



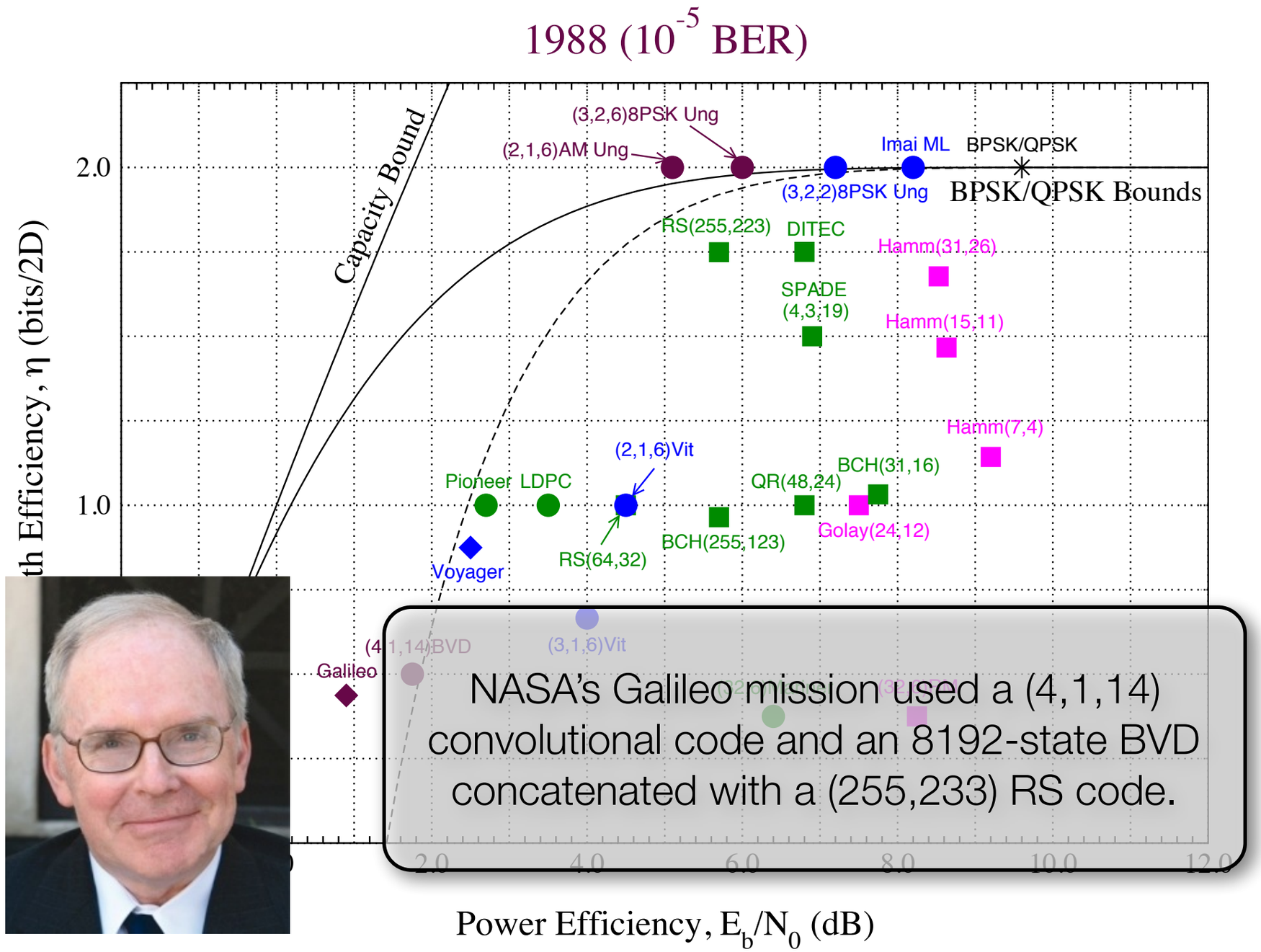
The Fourth Day



The Fourth Day

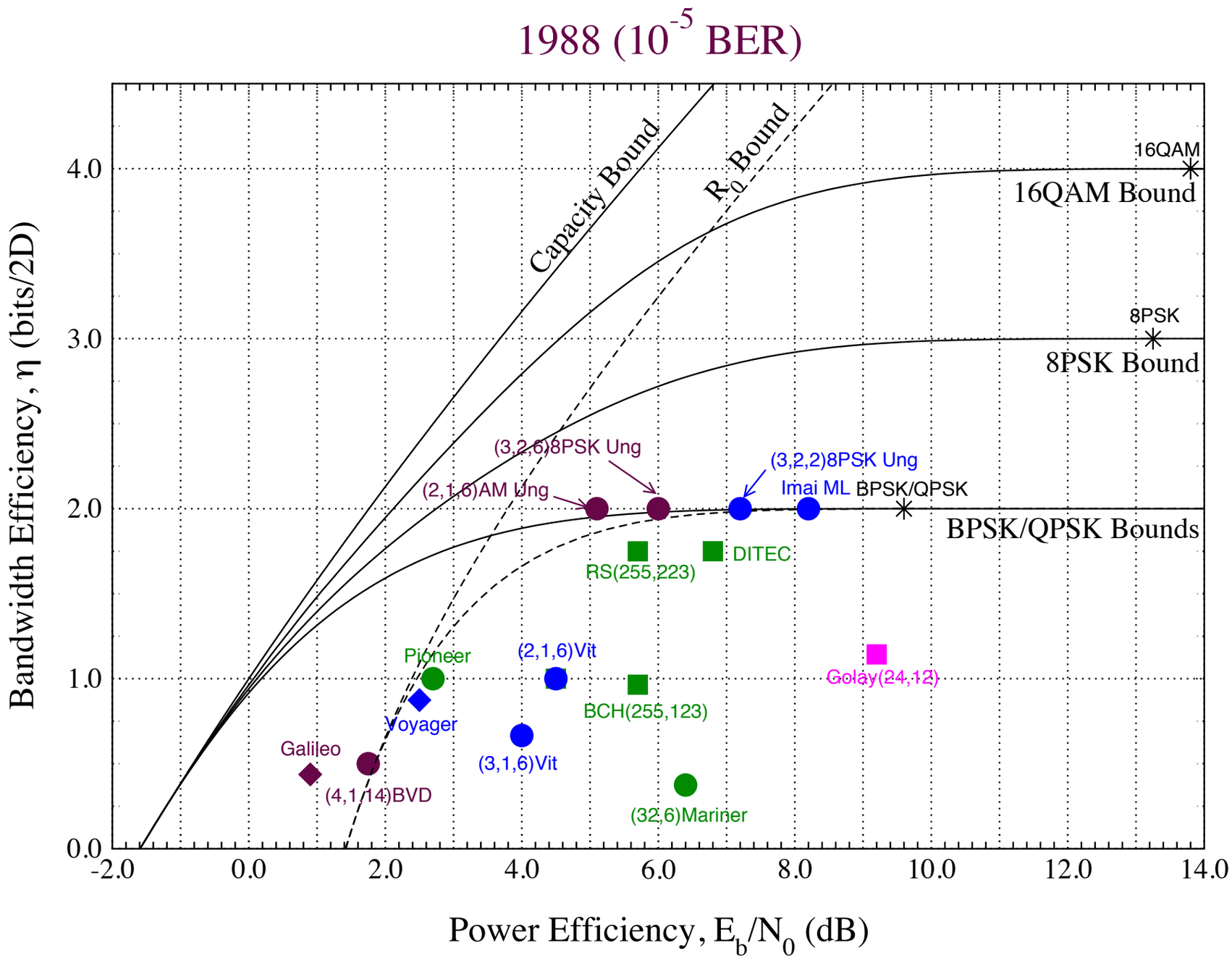


The Fourth Day

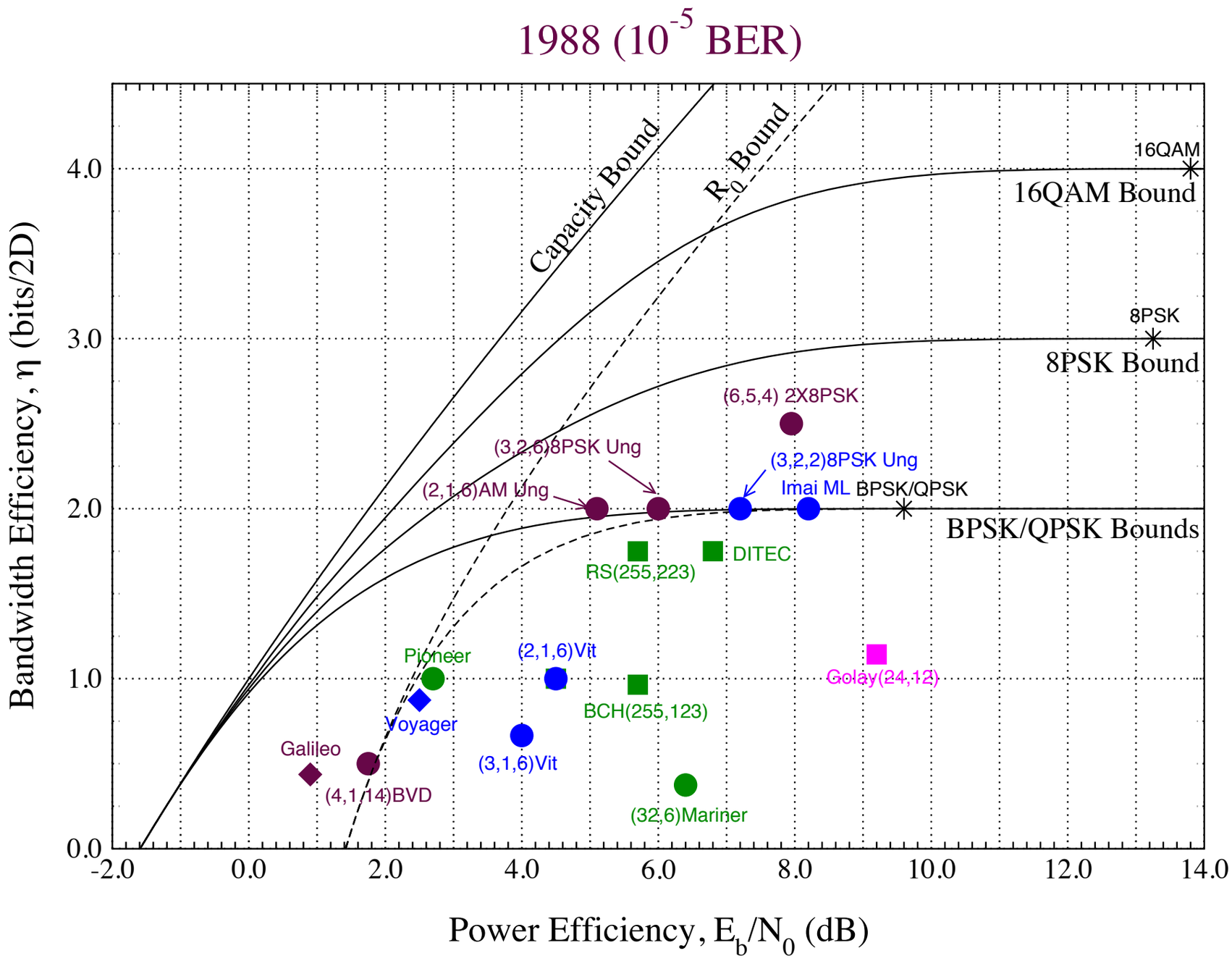


NASA's Galileo mission used a (4,1,14) convolutional code and an 8192-state BVD concatenated with a (255,233) RS code.

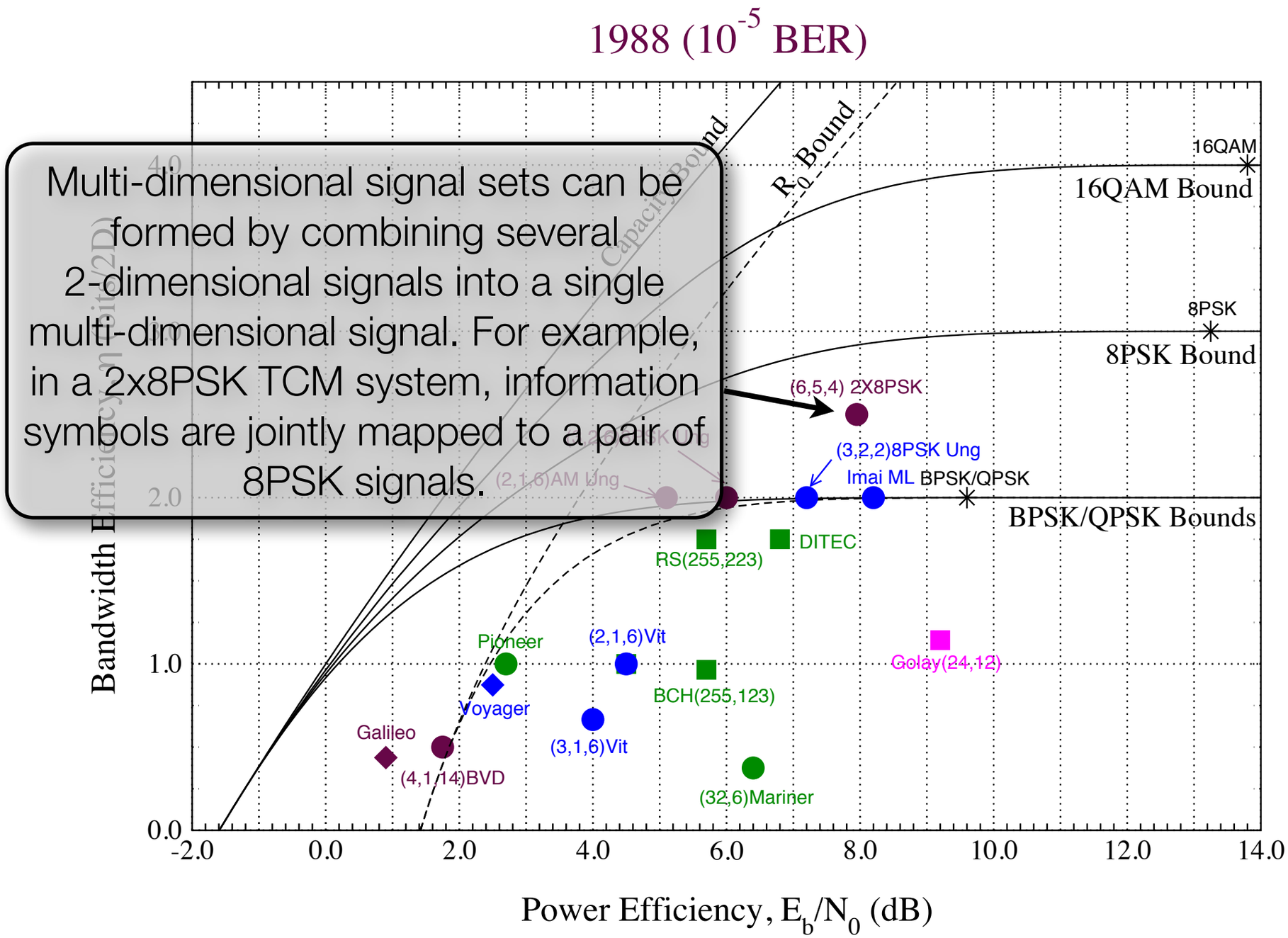
The Fourth Day



The Fourth Day

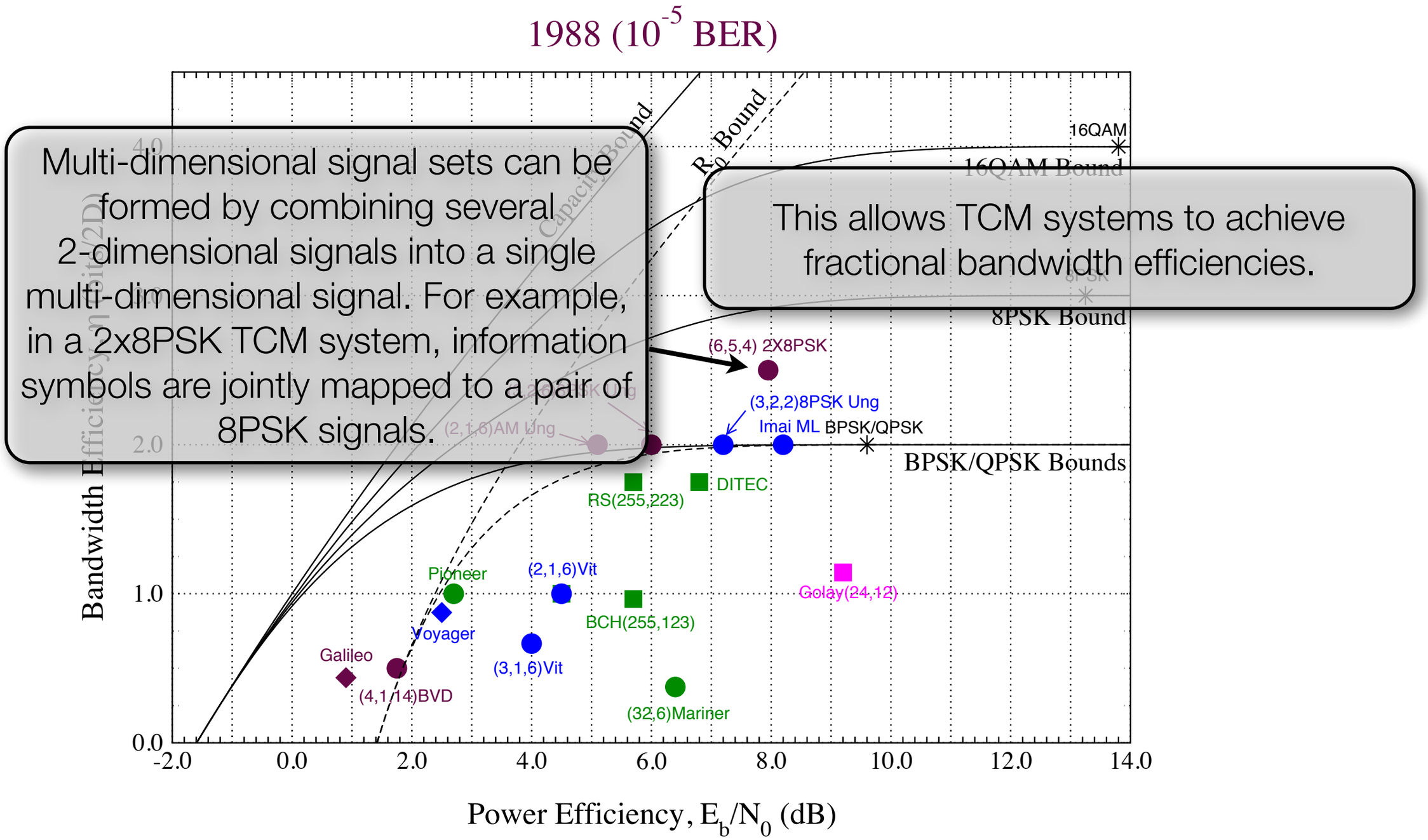


The Fourth Day

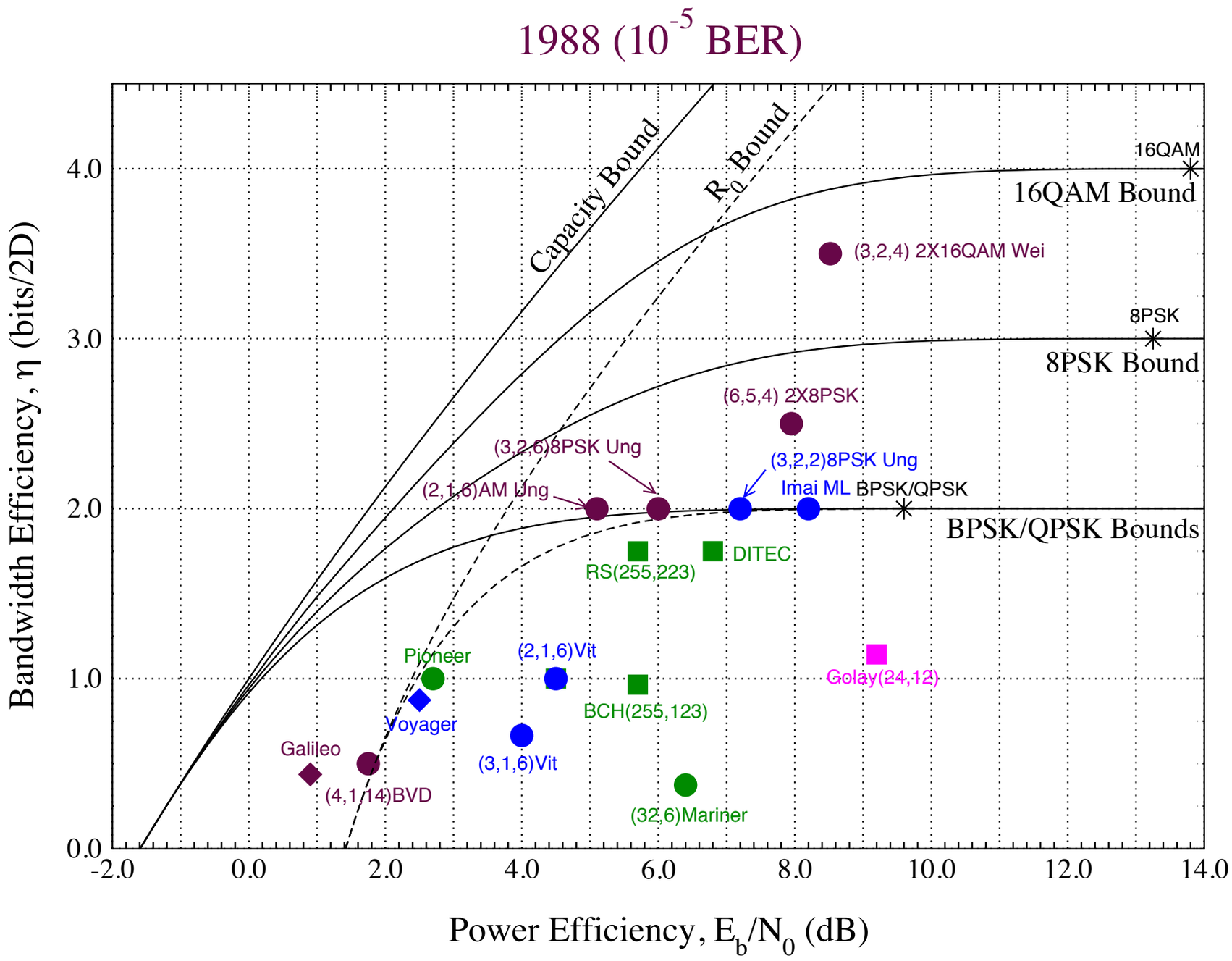


Multi-dimensional signal sets can be formed by combining several 2-dimensional signals into a single multi-dimensional signal. For example, in a 2x8PSK TCM system, information symbols are jointly mapped to a pair of 8PSK signals.

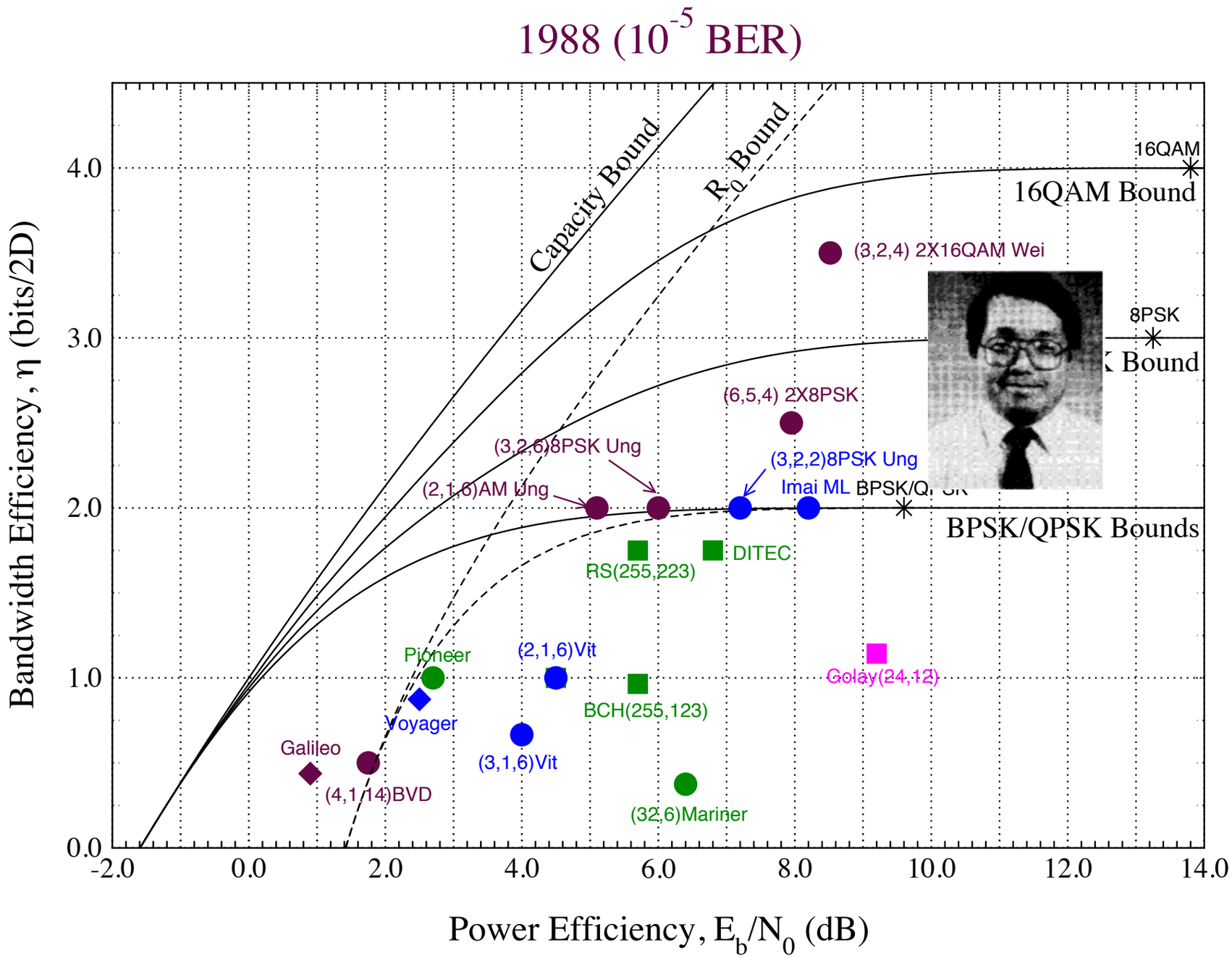
The Fourth Day



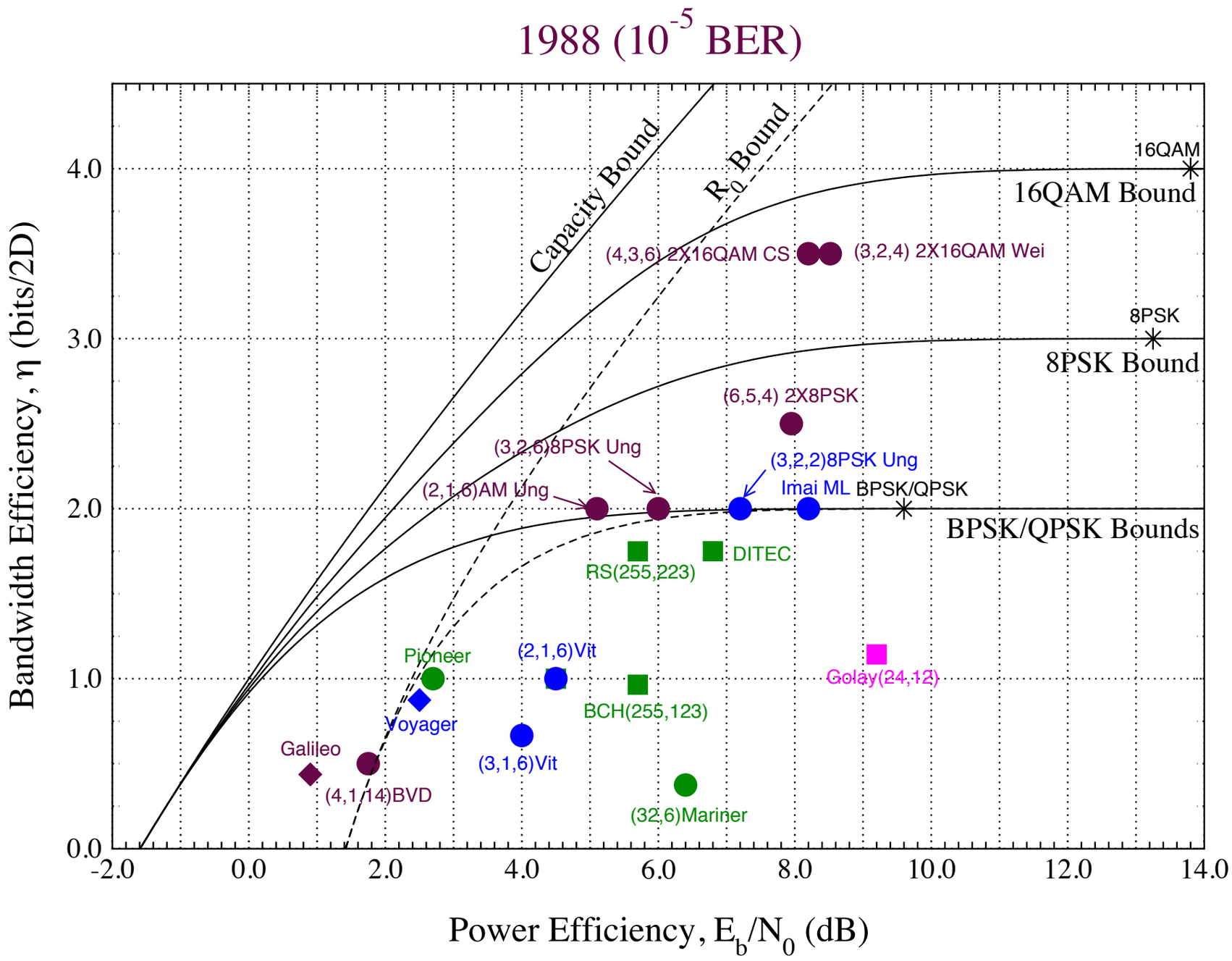
The Fourth Day



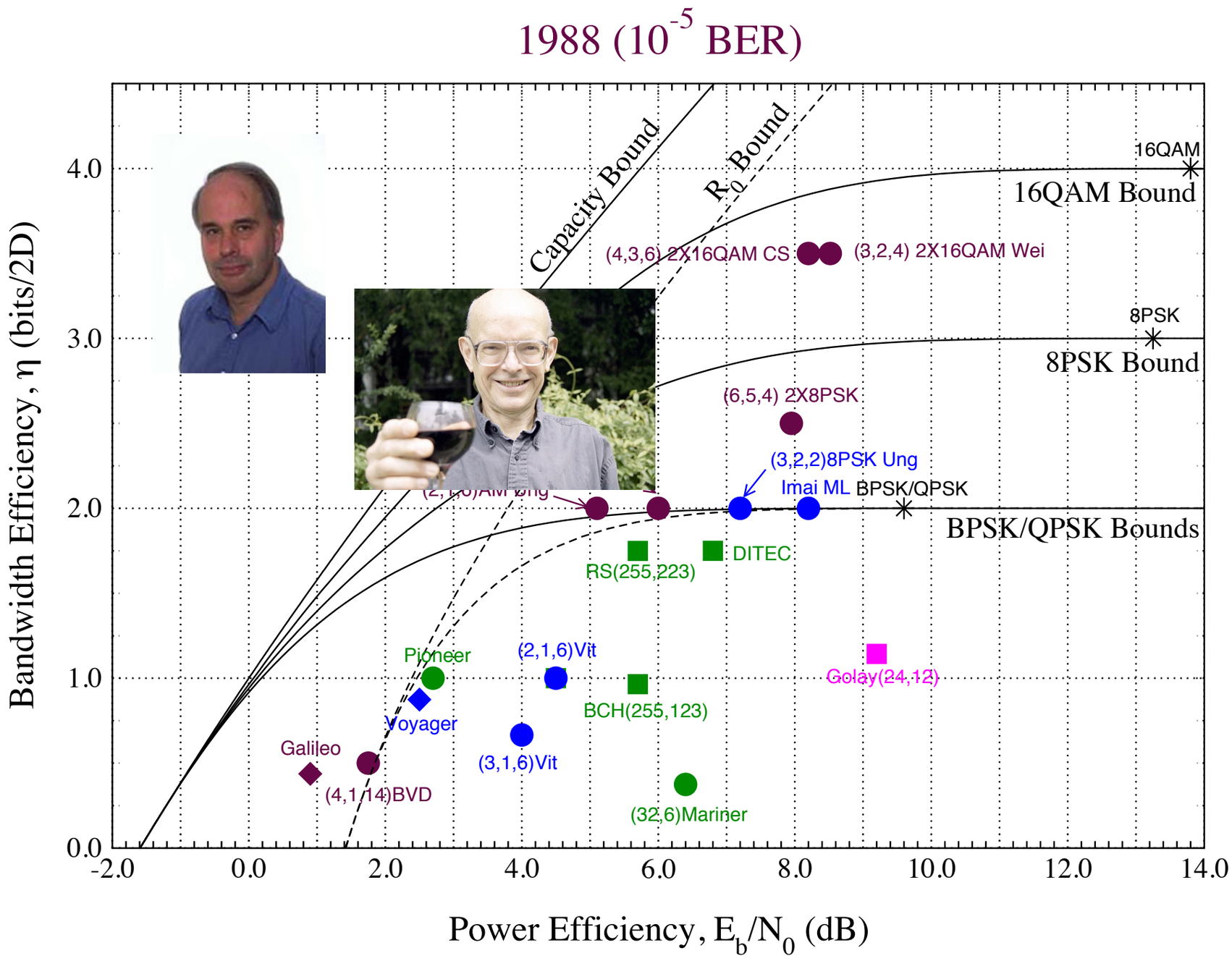
The Fourth Day



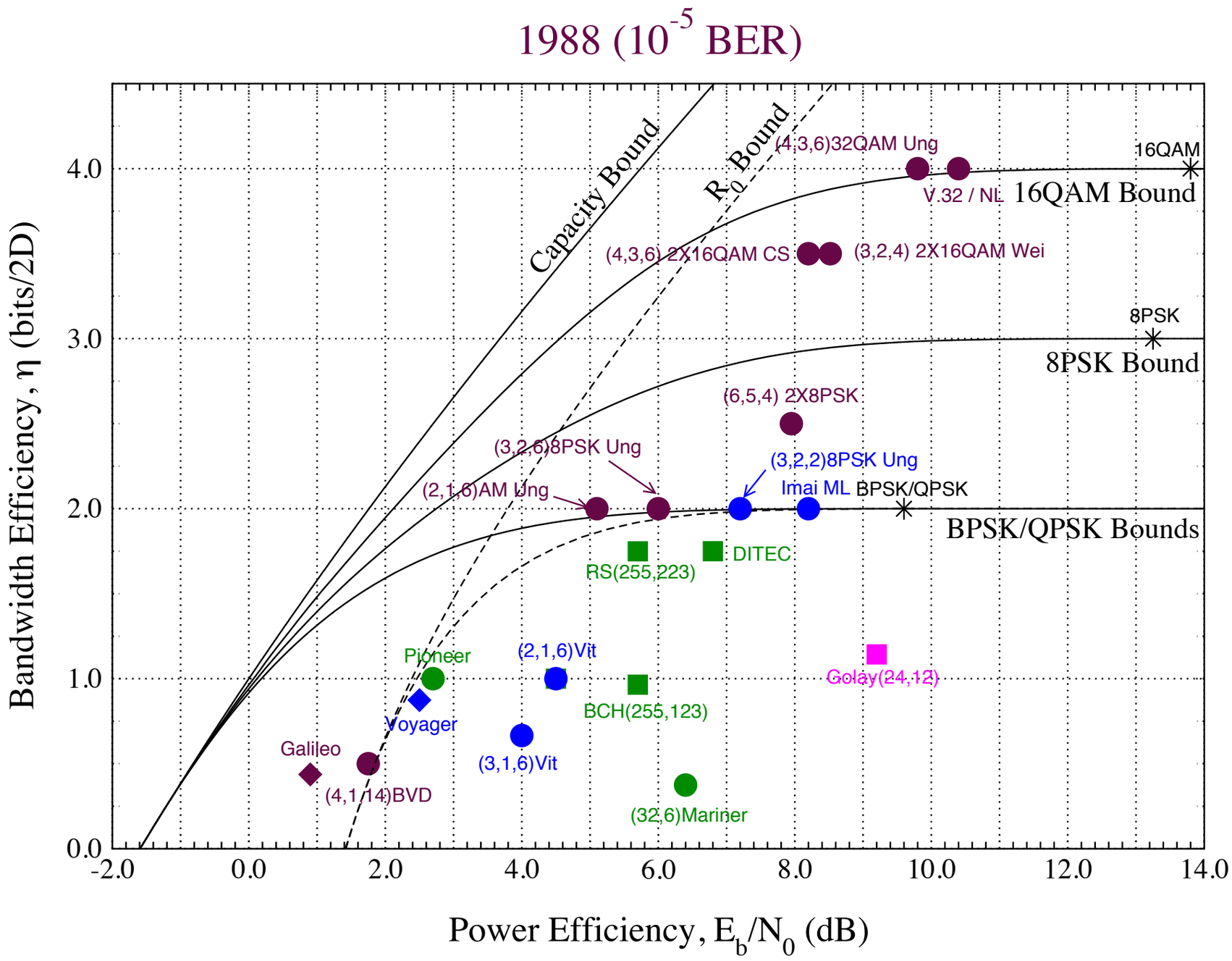
The Fourth Day



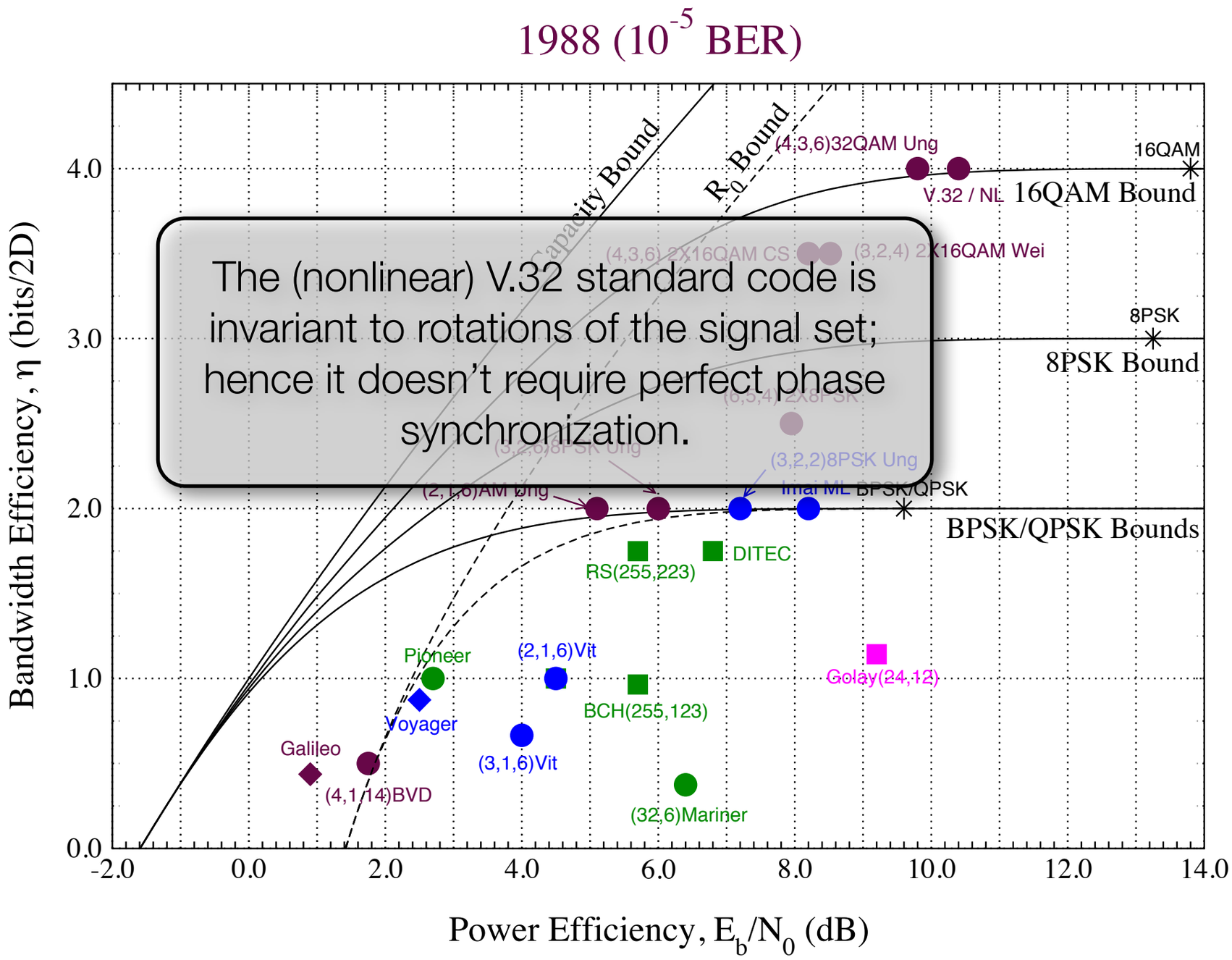
The Fourth Day



The Fourth Day

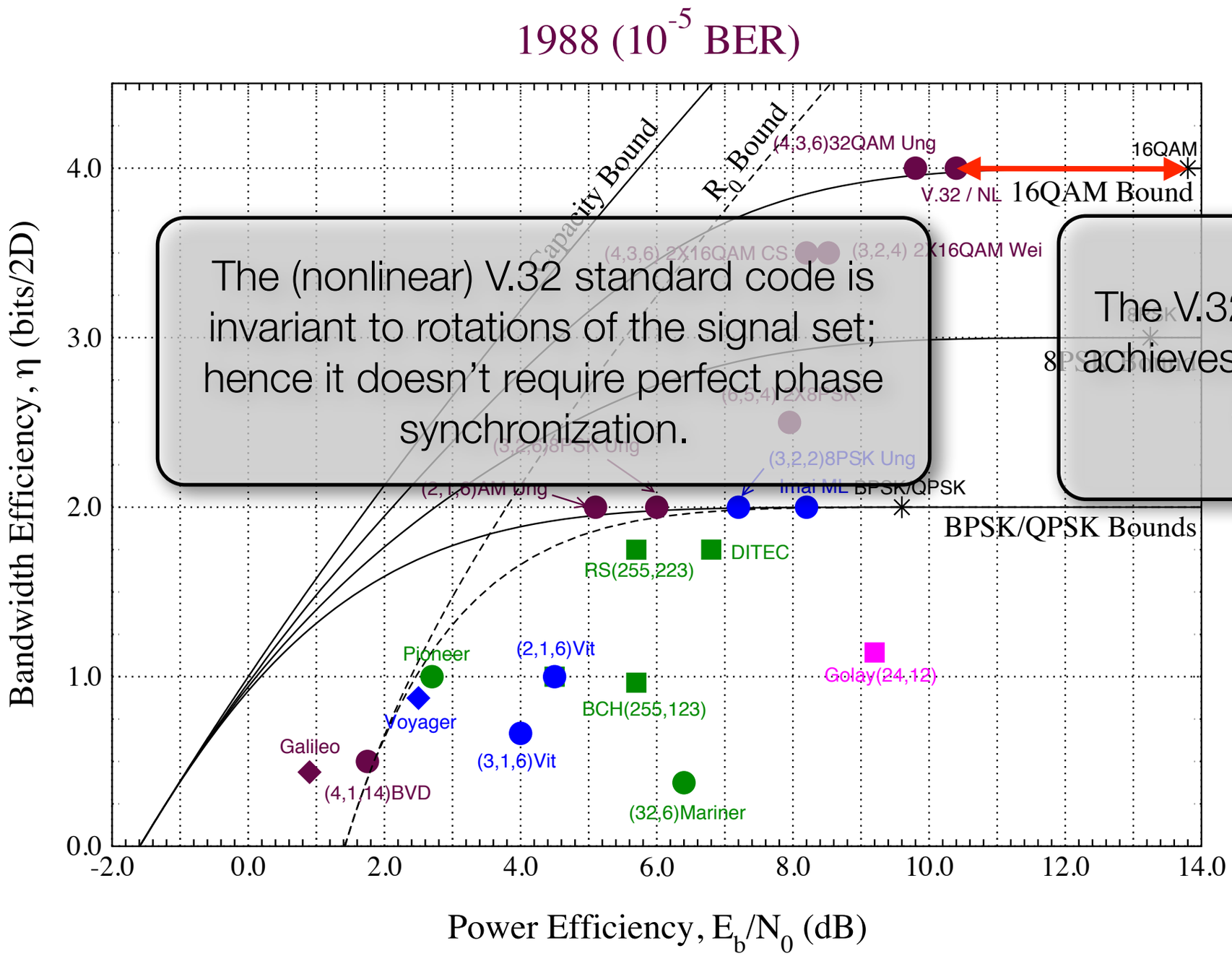


The Fourth Day



The (nonlinear) V.32 standard code is invariant to rotations of the signal set; hence it doesn't require perfect phase synchronization.

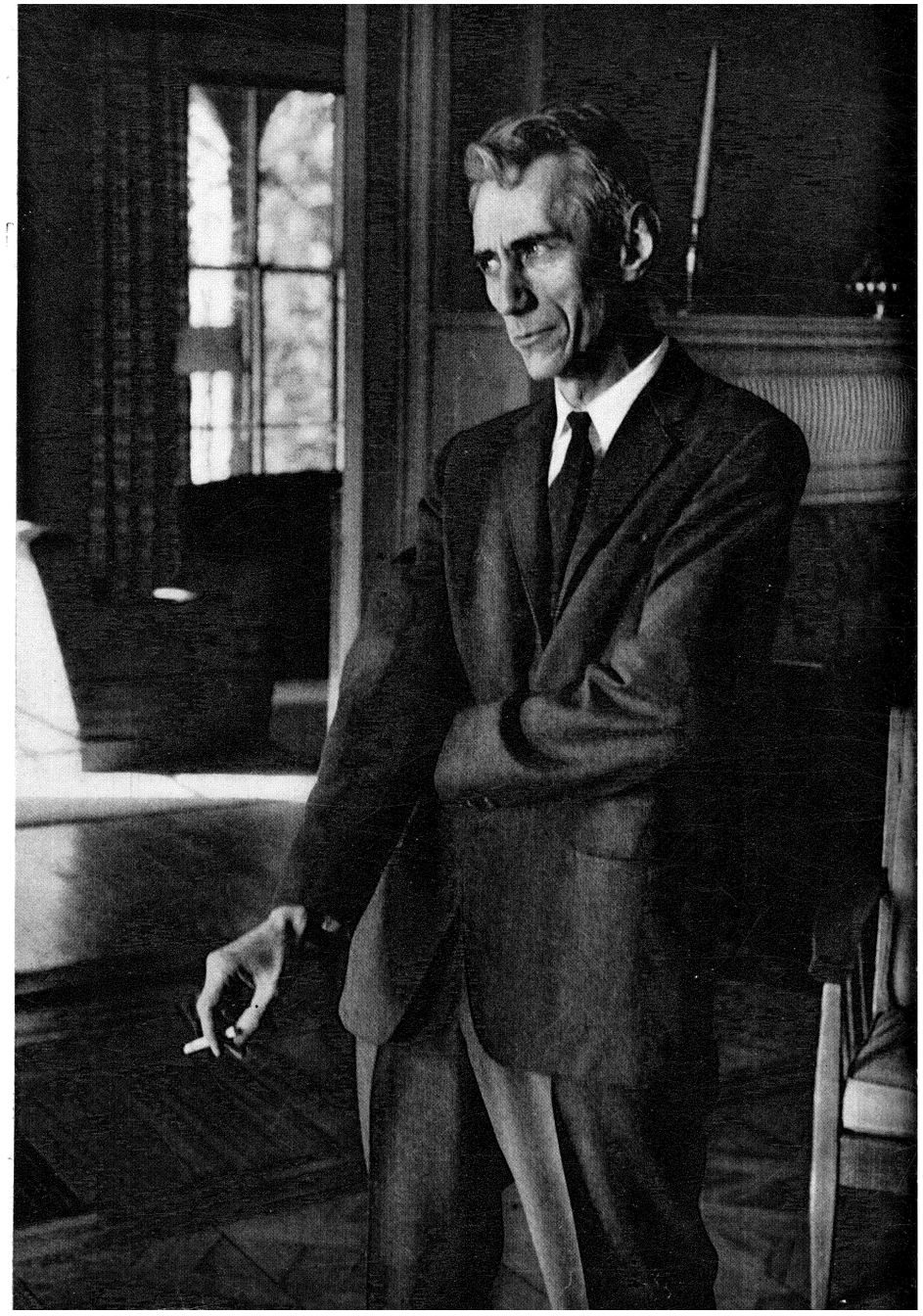
The Fourth Day



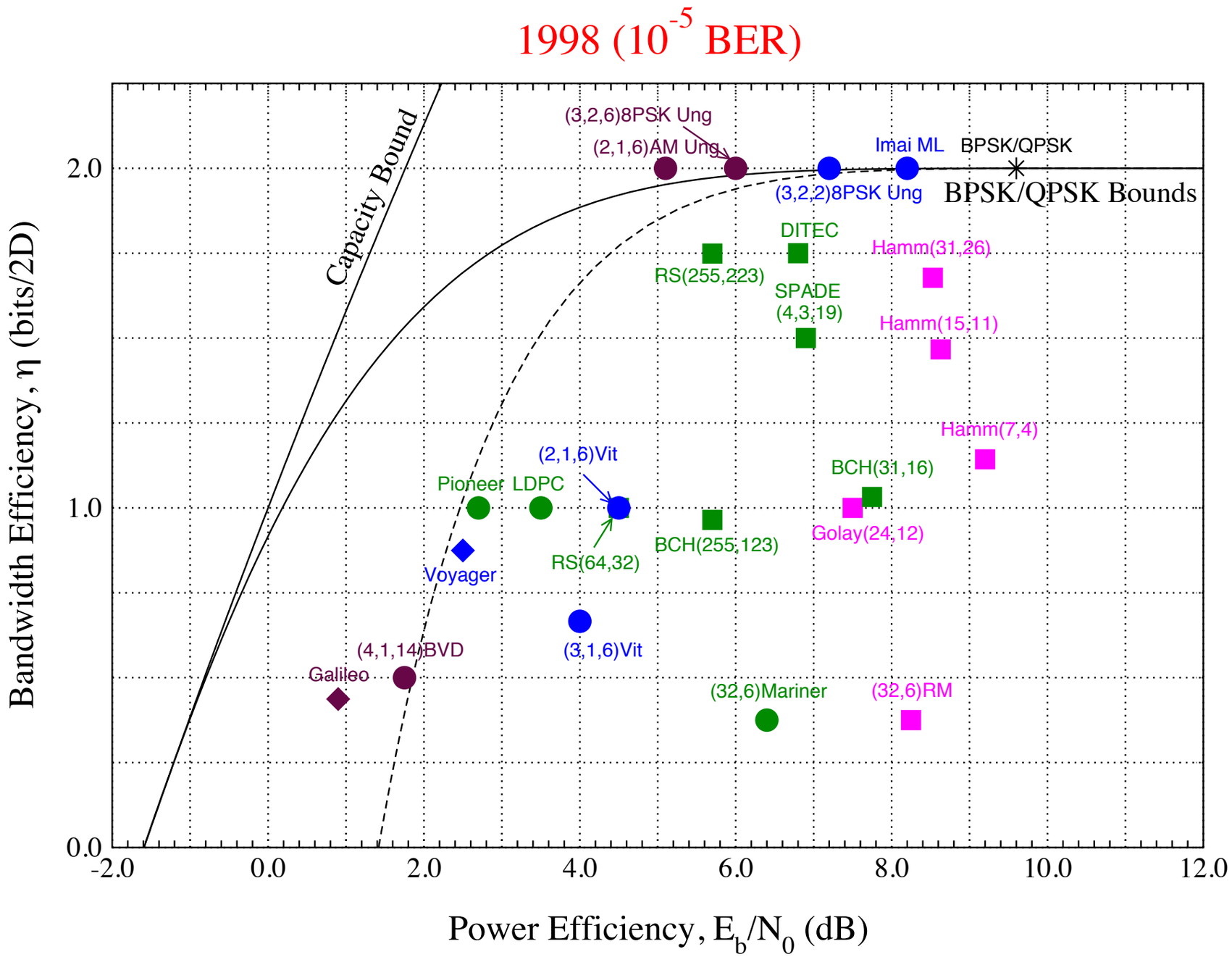
The (nonlinear) V.32 standard code is invariant to rotations of the signal set; hence it doesn't require perfect phase synchronization.

The V.32 standard code achieves a coding gain of 3.47 dB.

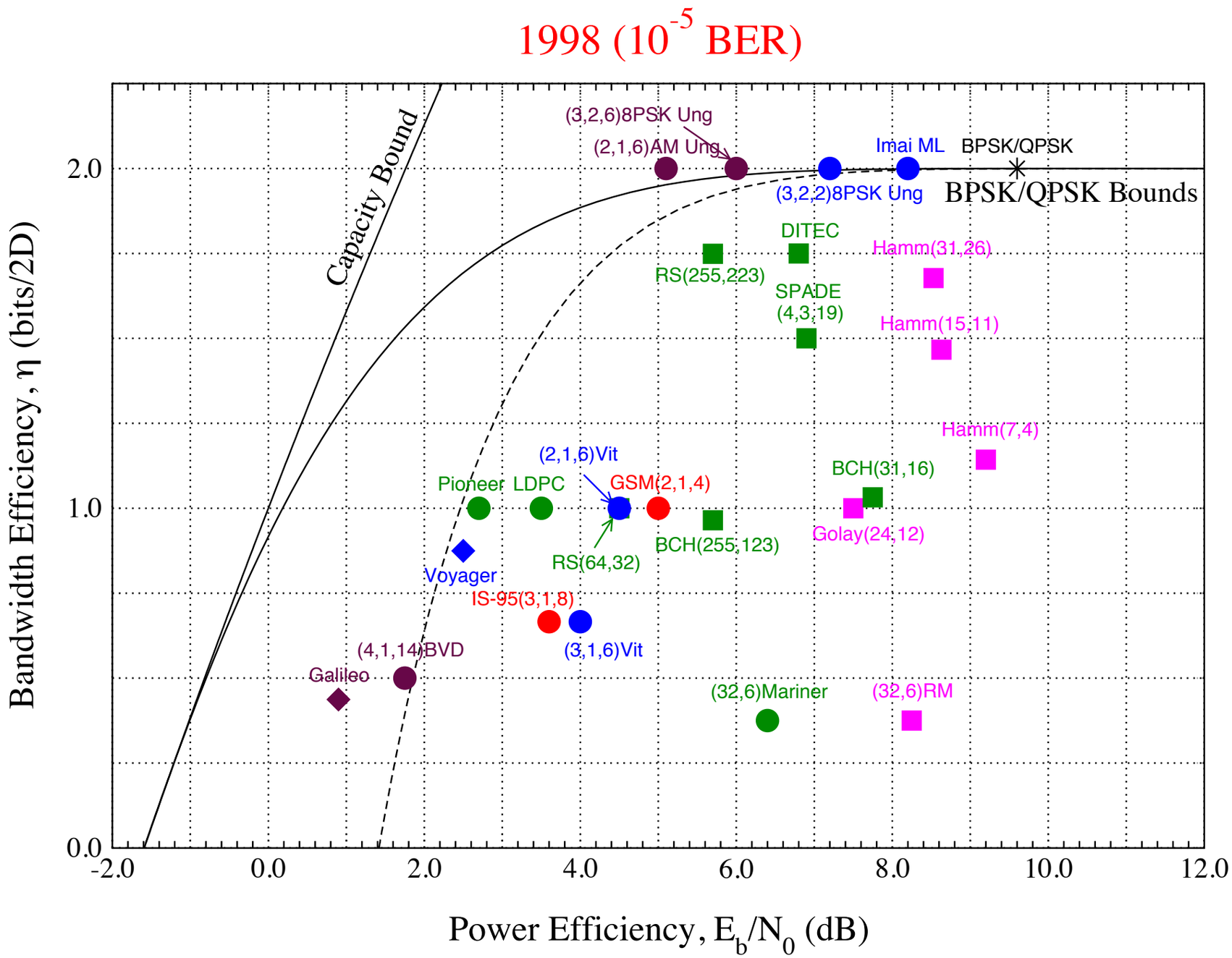
The Fifth Day



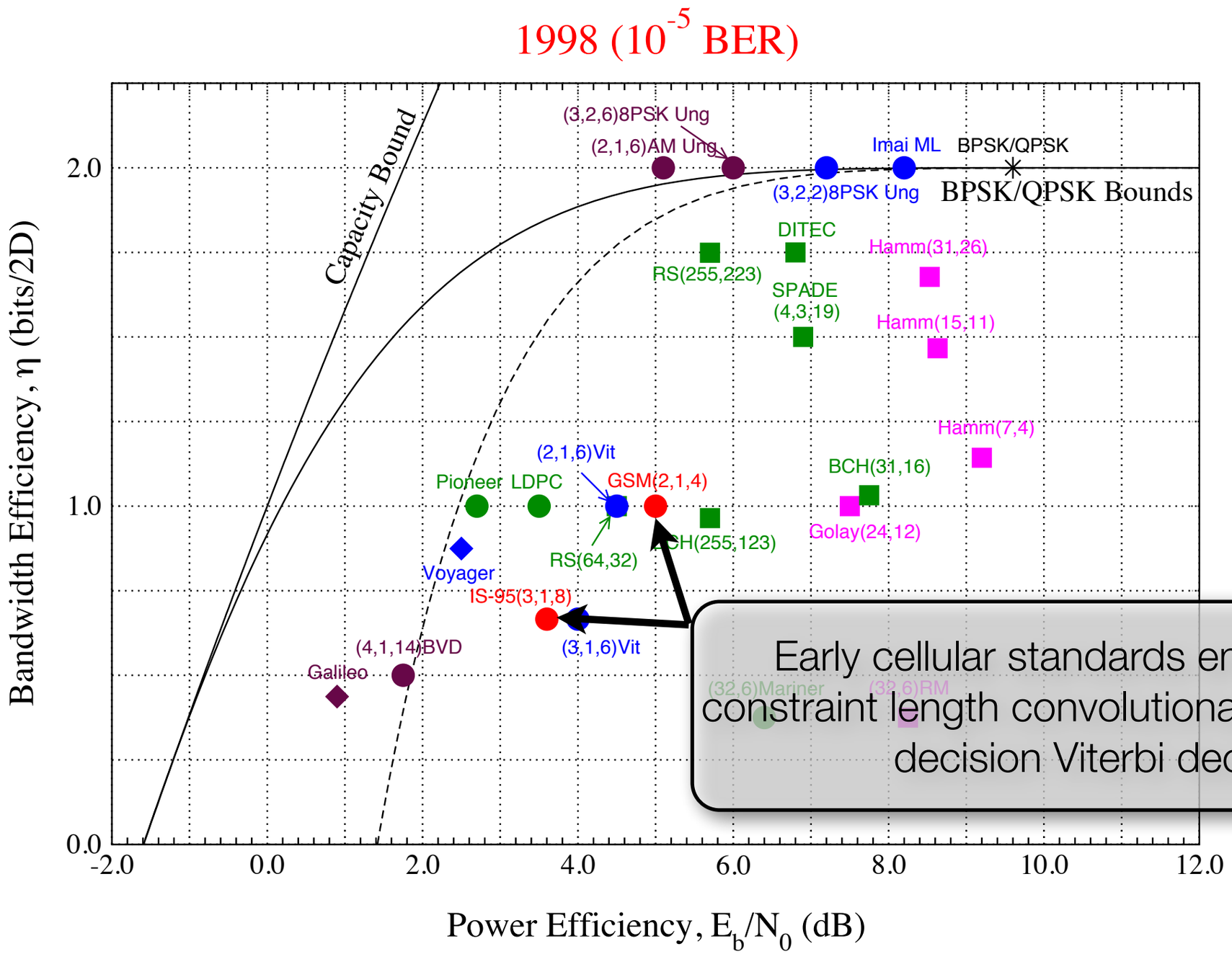
The Fifth Day



The Fifth Day

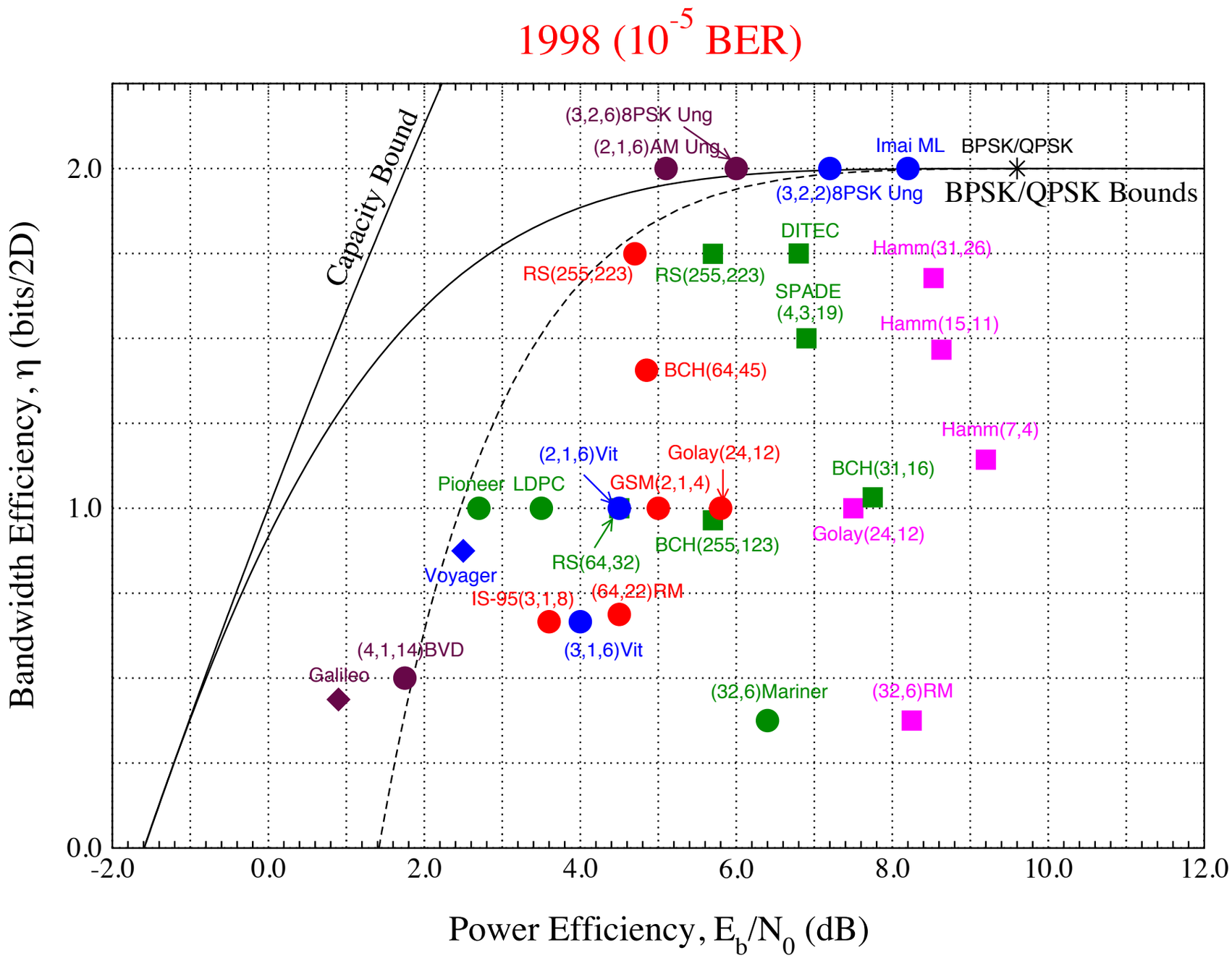


The Fifth Day

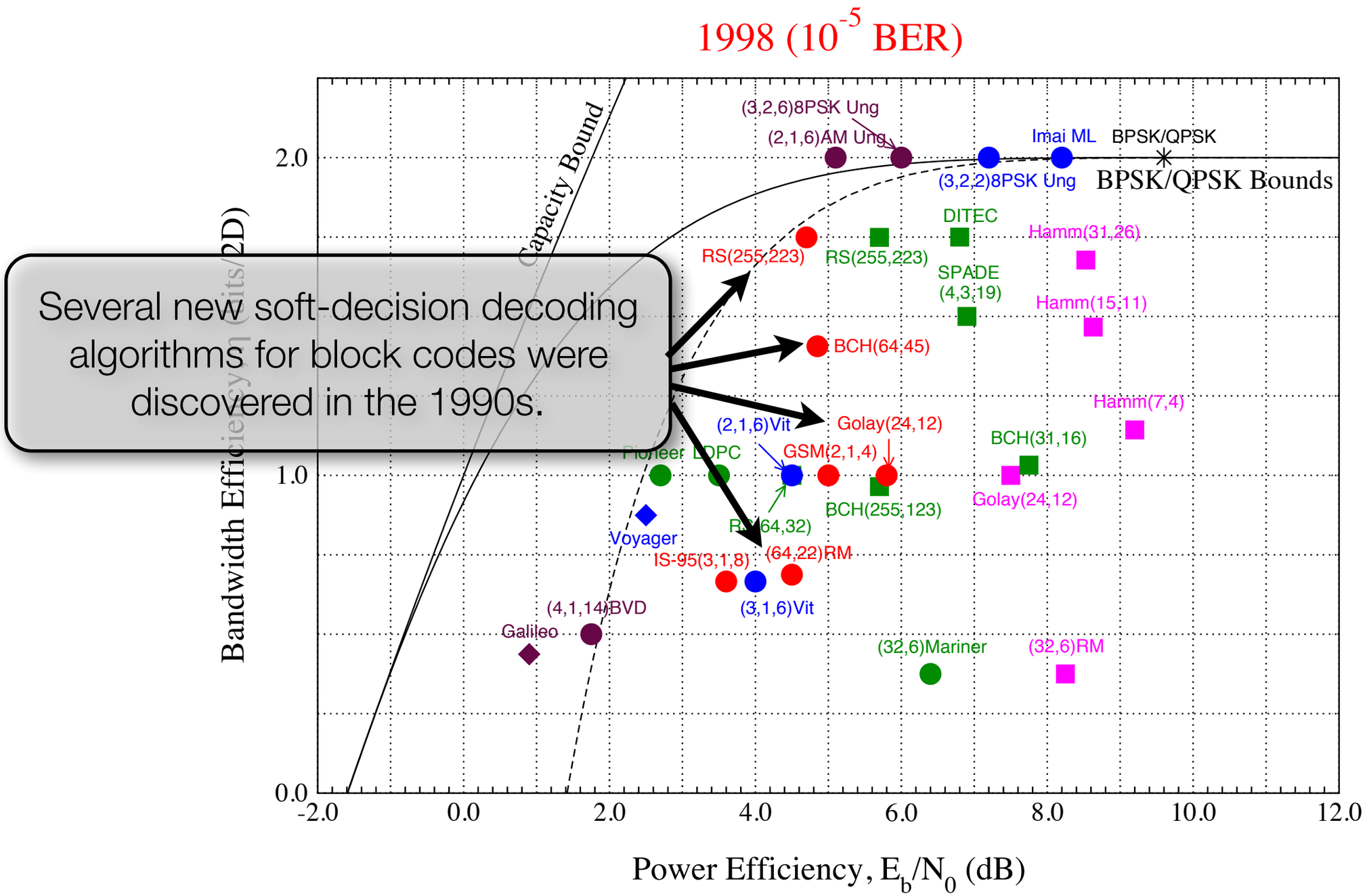


Early cellular standards employed short constraint length convolutional codes with soft-decision Viterbi decoding.

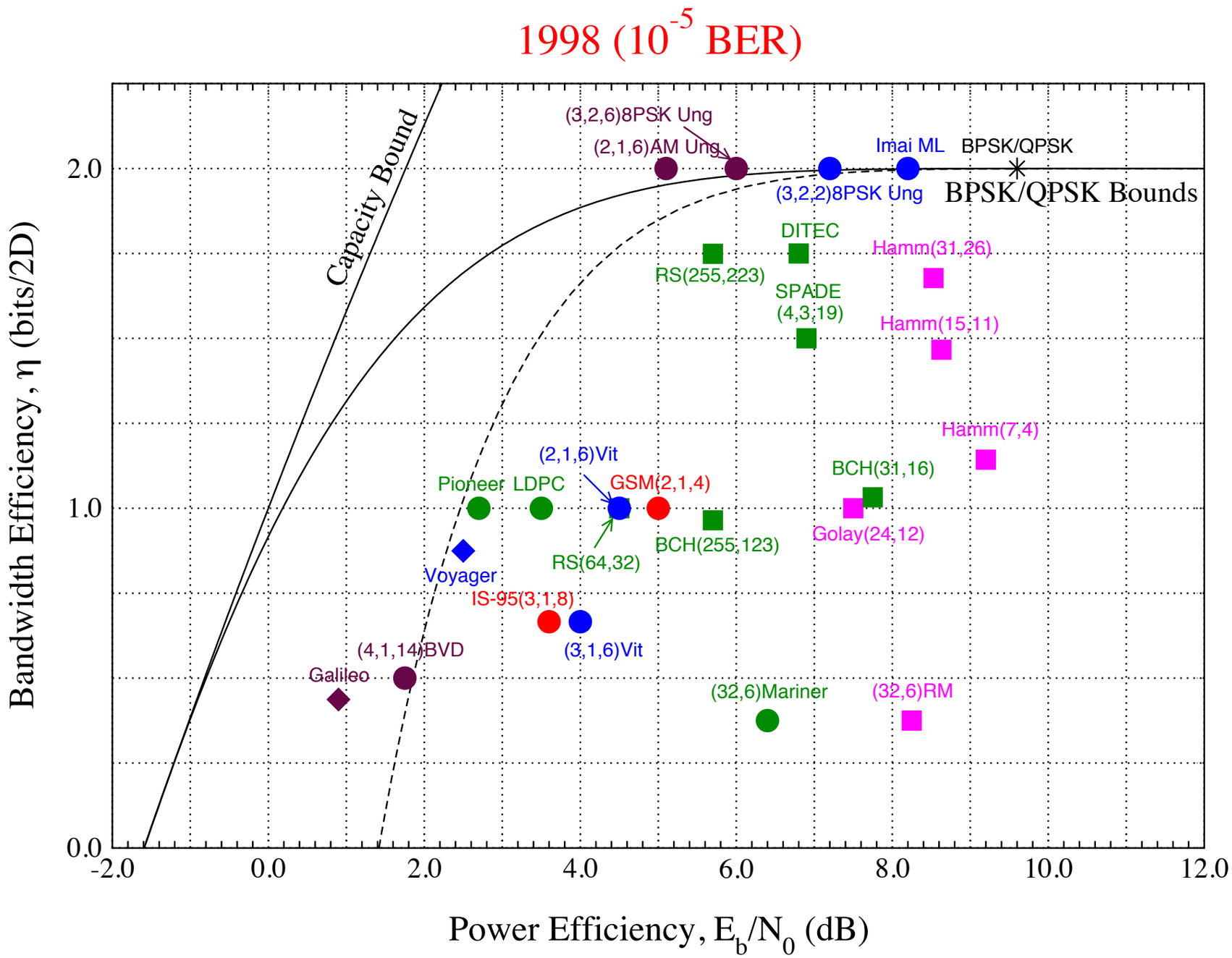
The Fifth Day



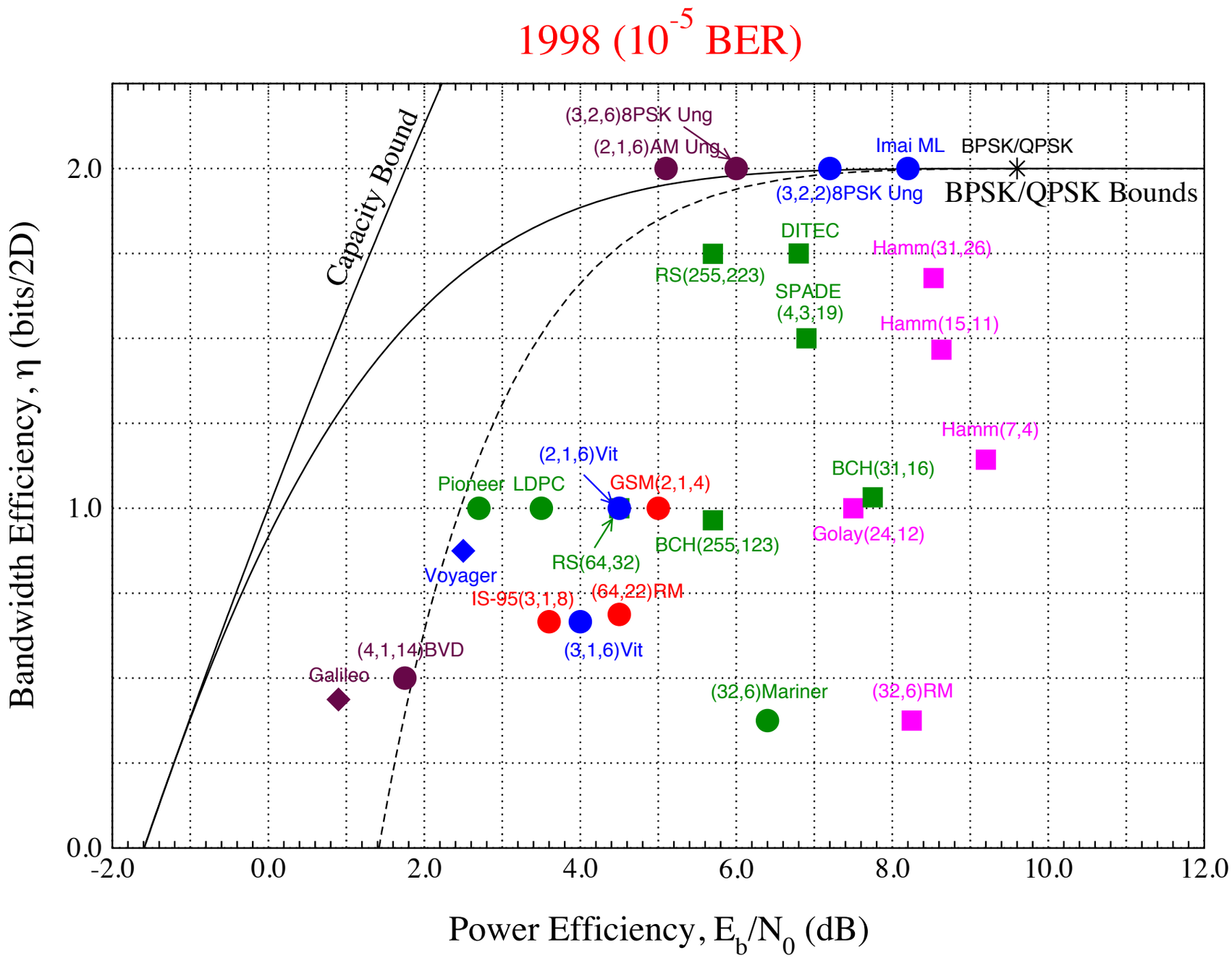
The Fifth Day



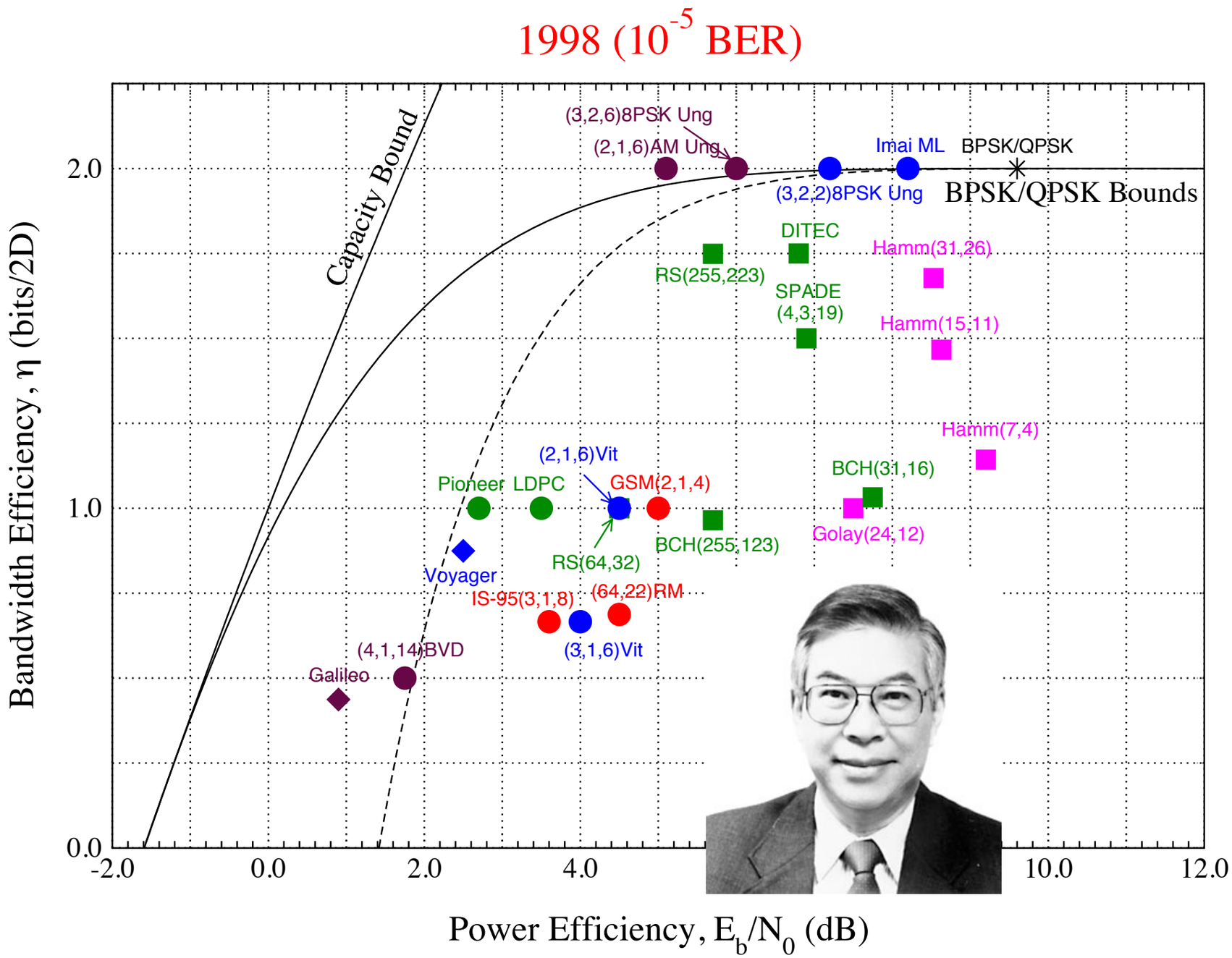
The Fifth Day



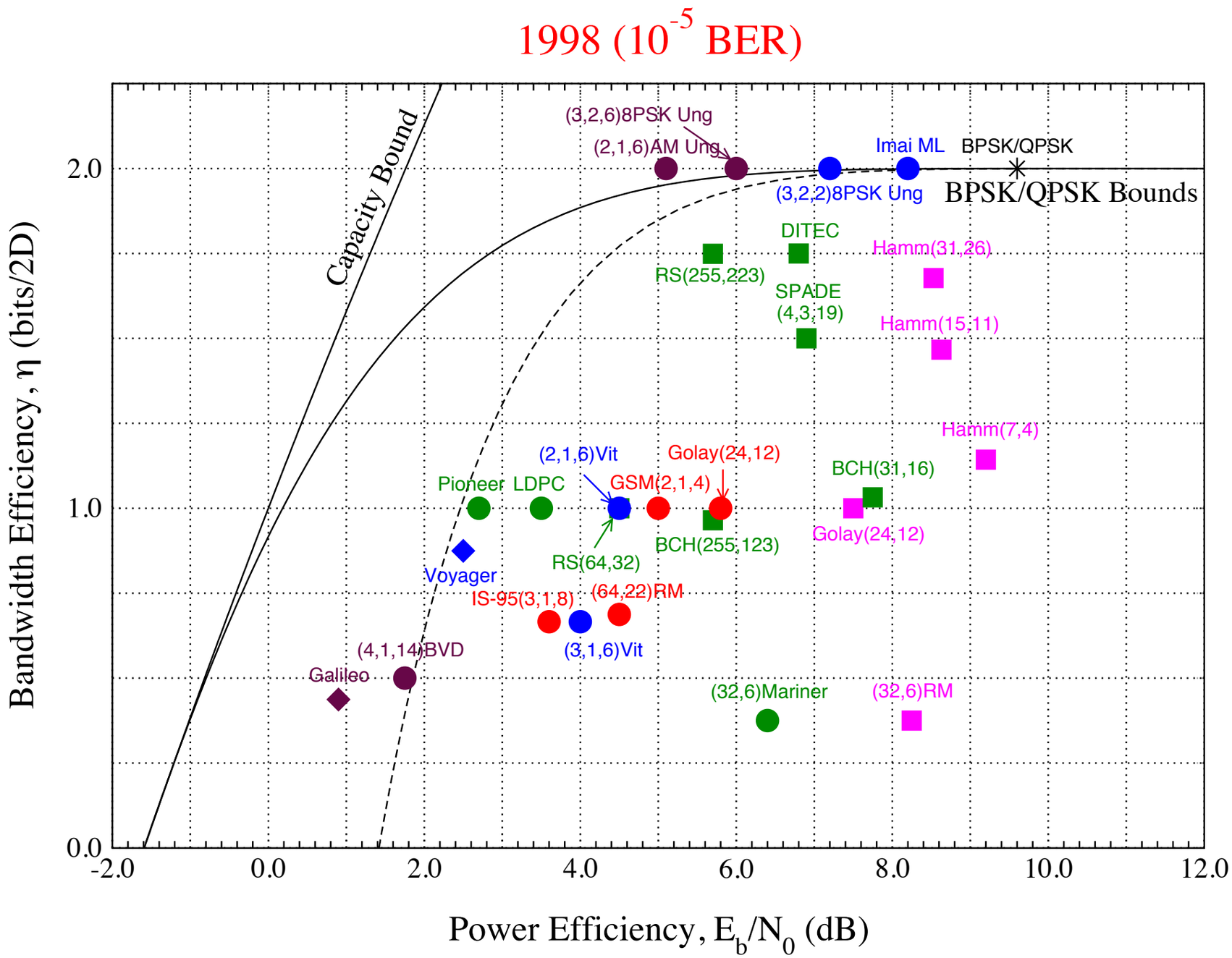
The Fifth Day



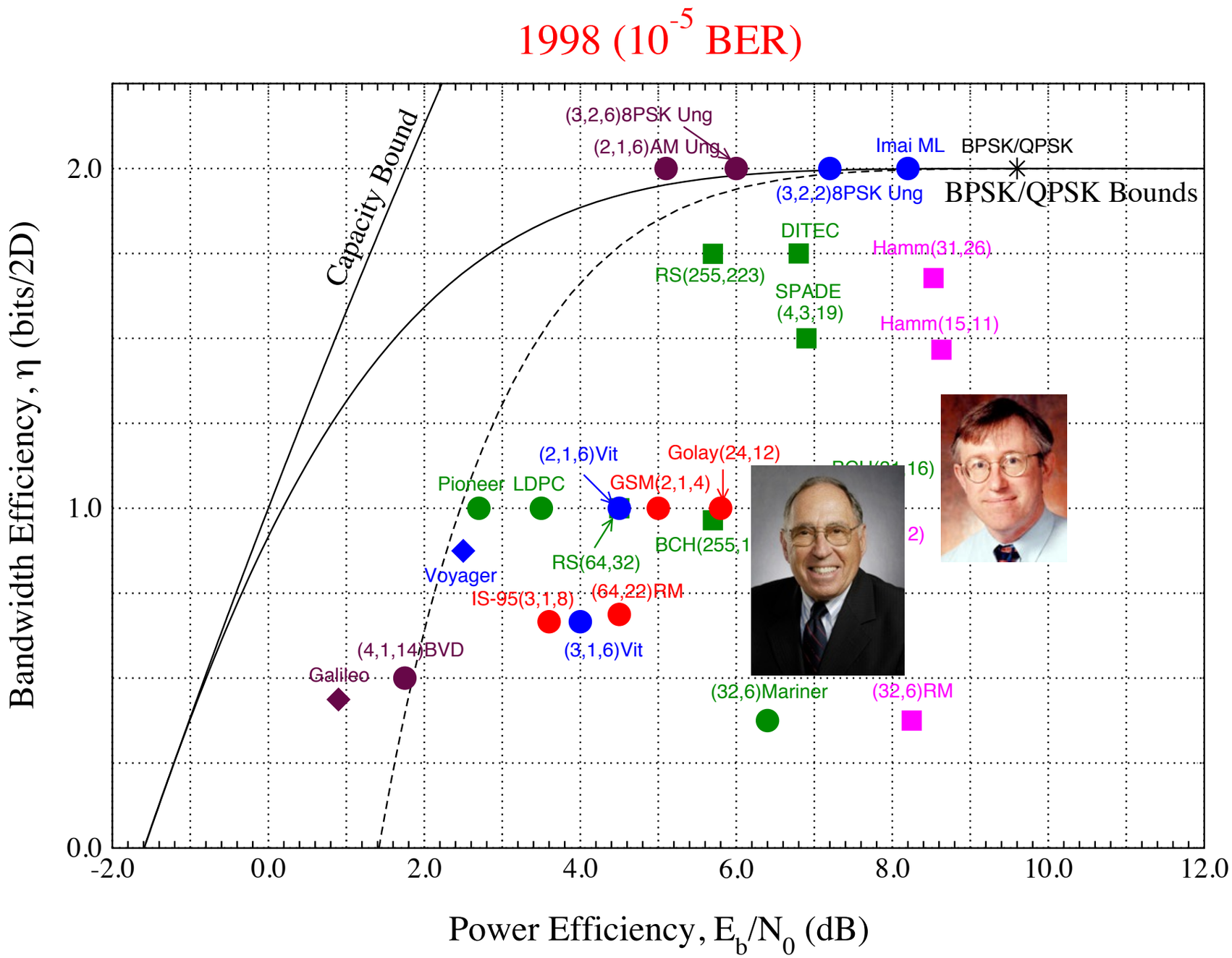
The Fifth Day



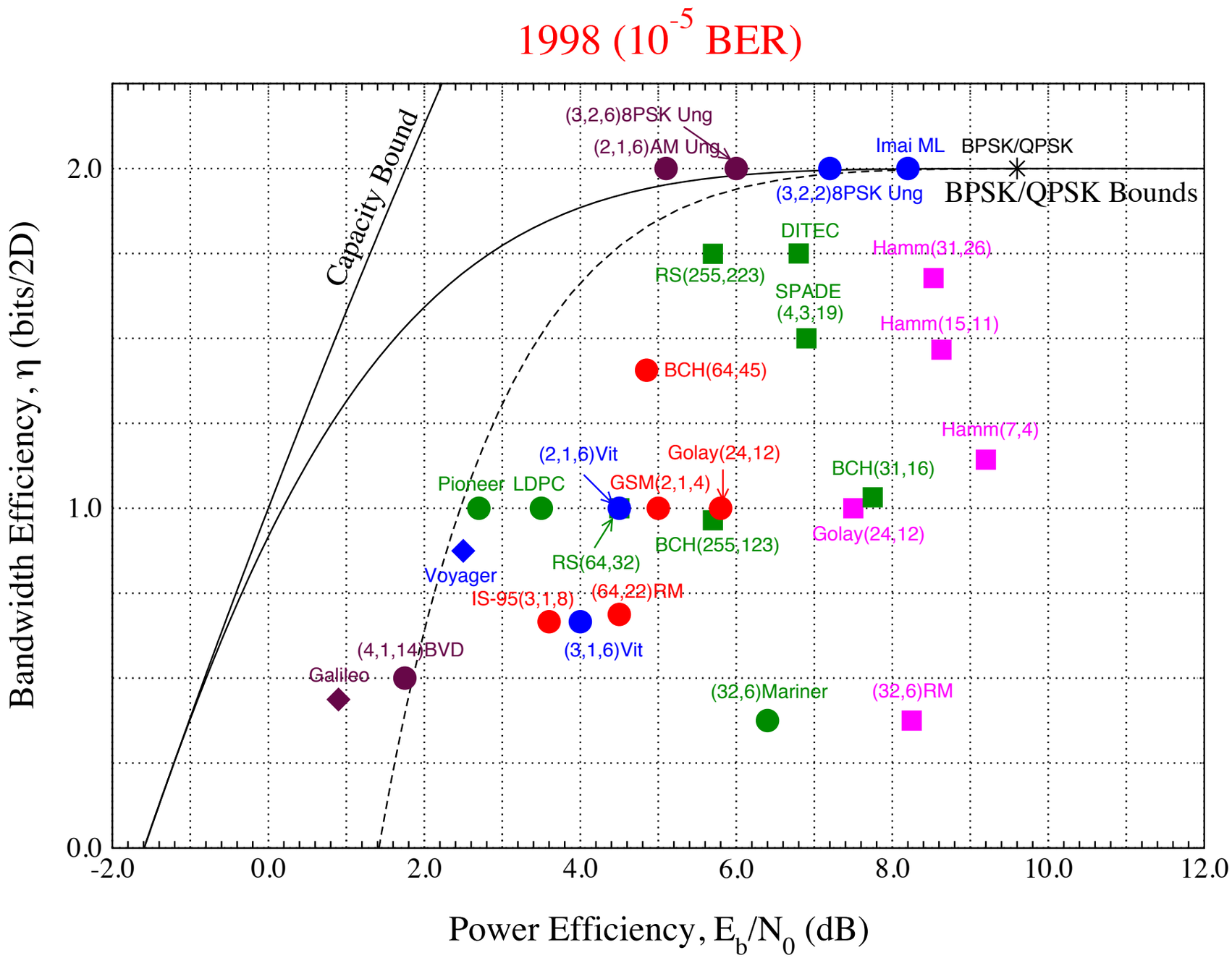
The Fifth Day



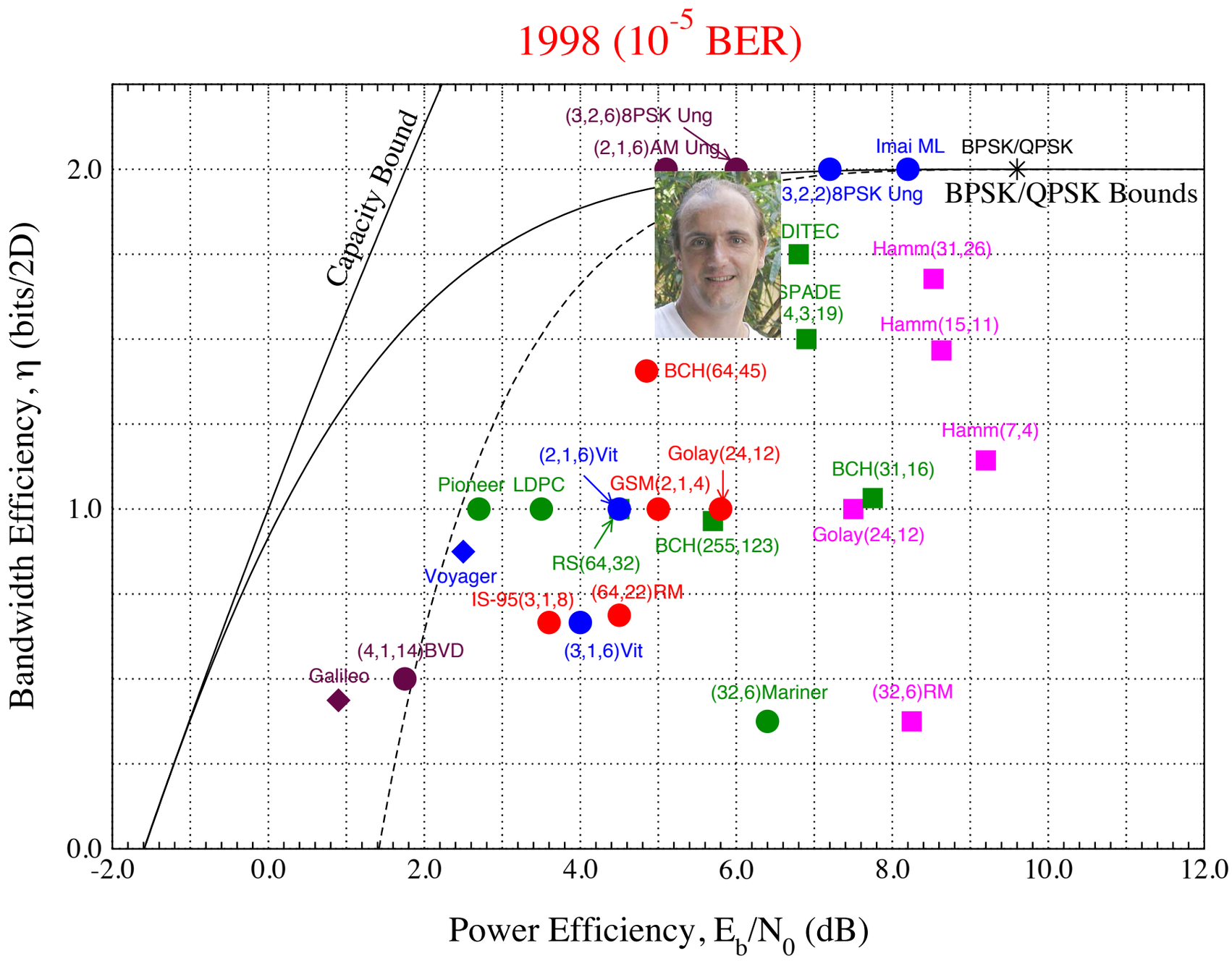
The Fifth Day



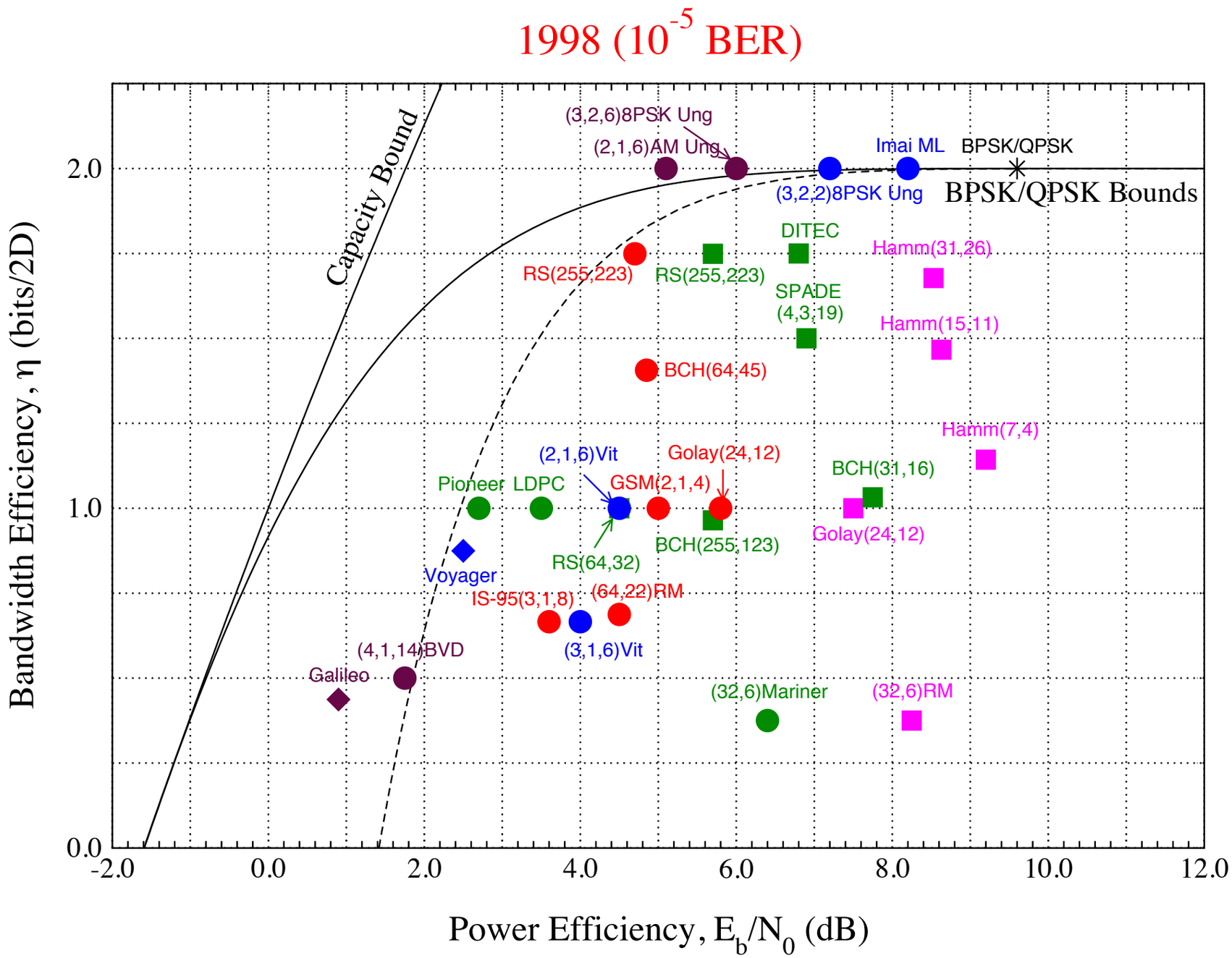
The Fifth Day



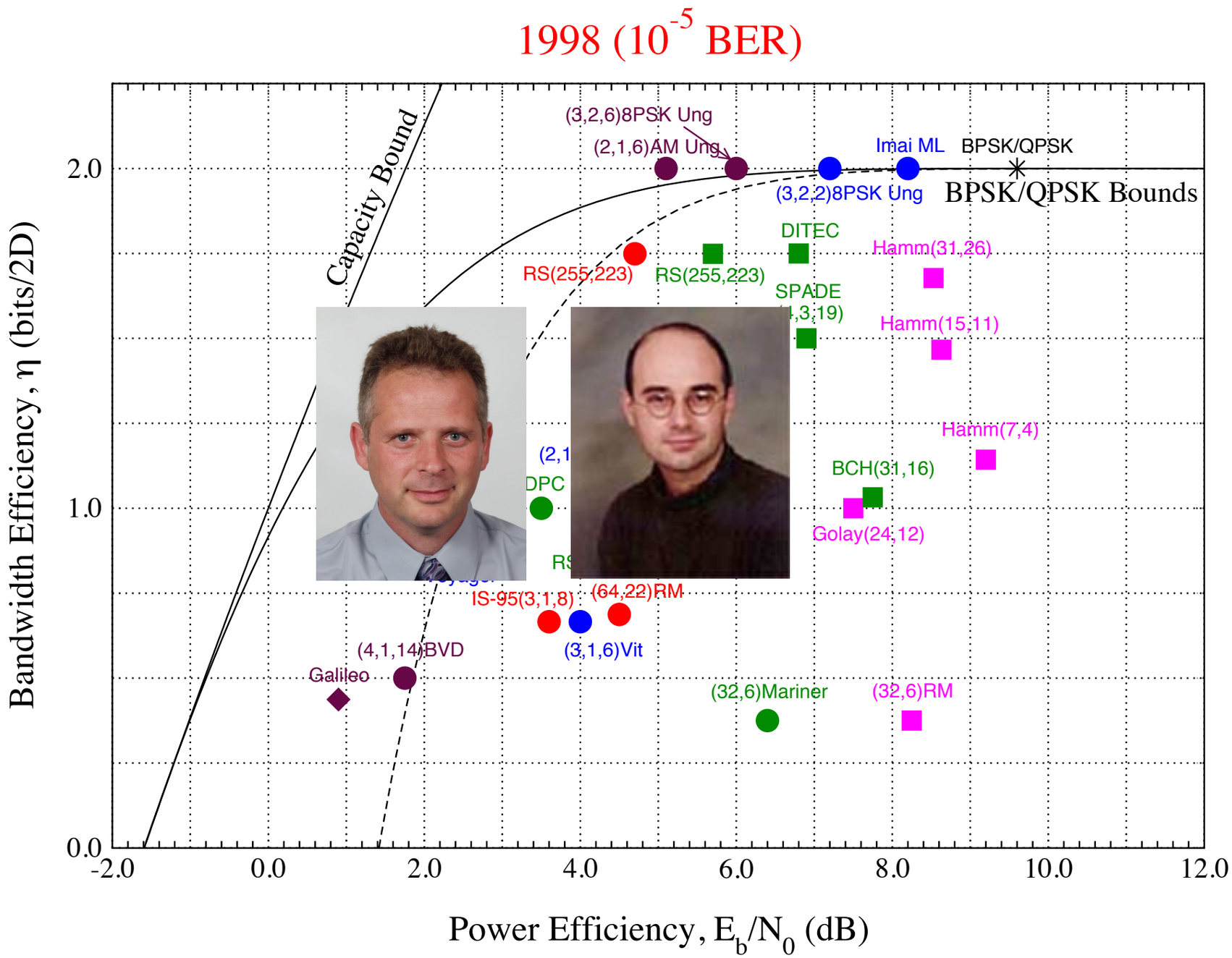
The Fifth Day



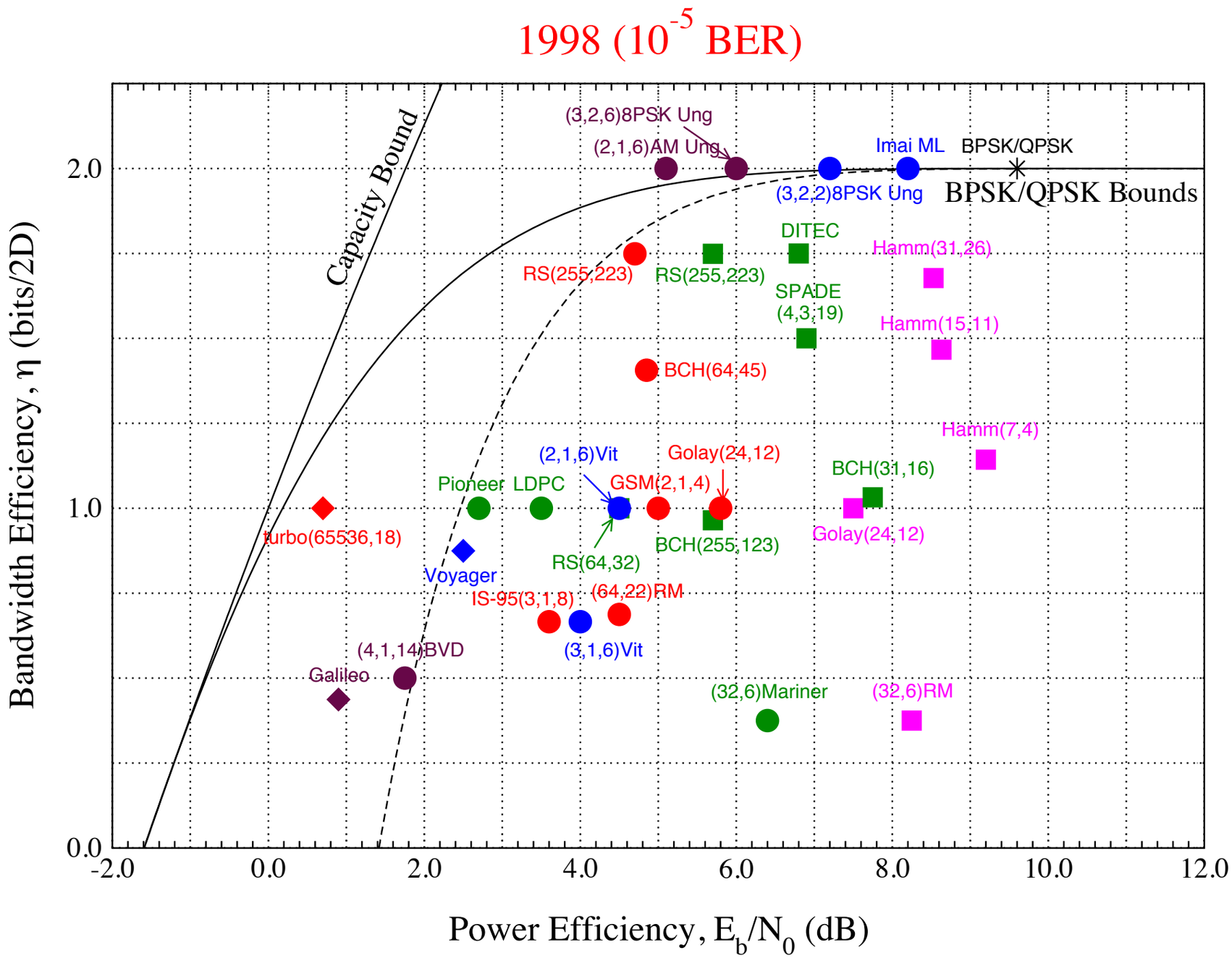
The Fifth Day



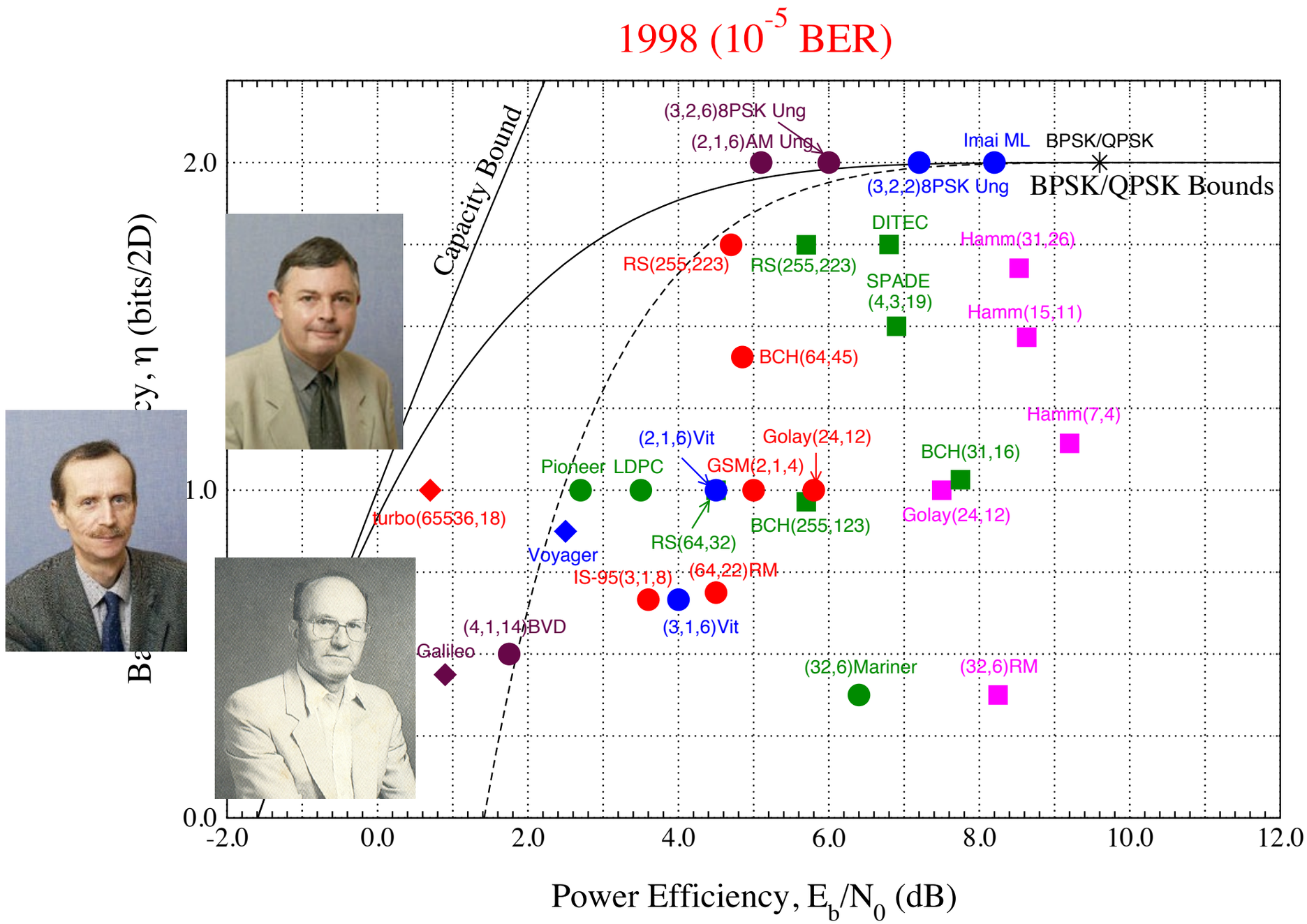
The Fifth Day



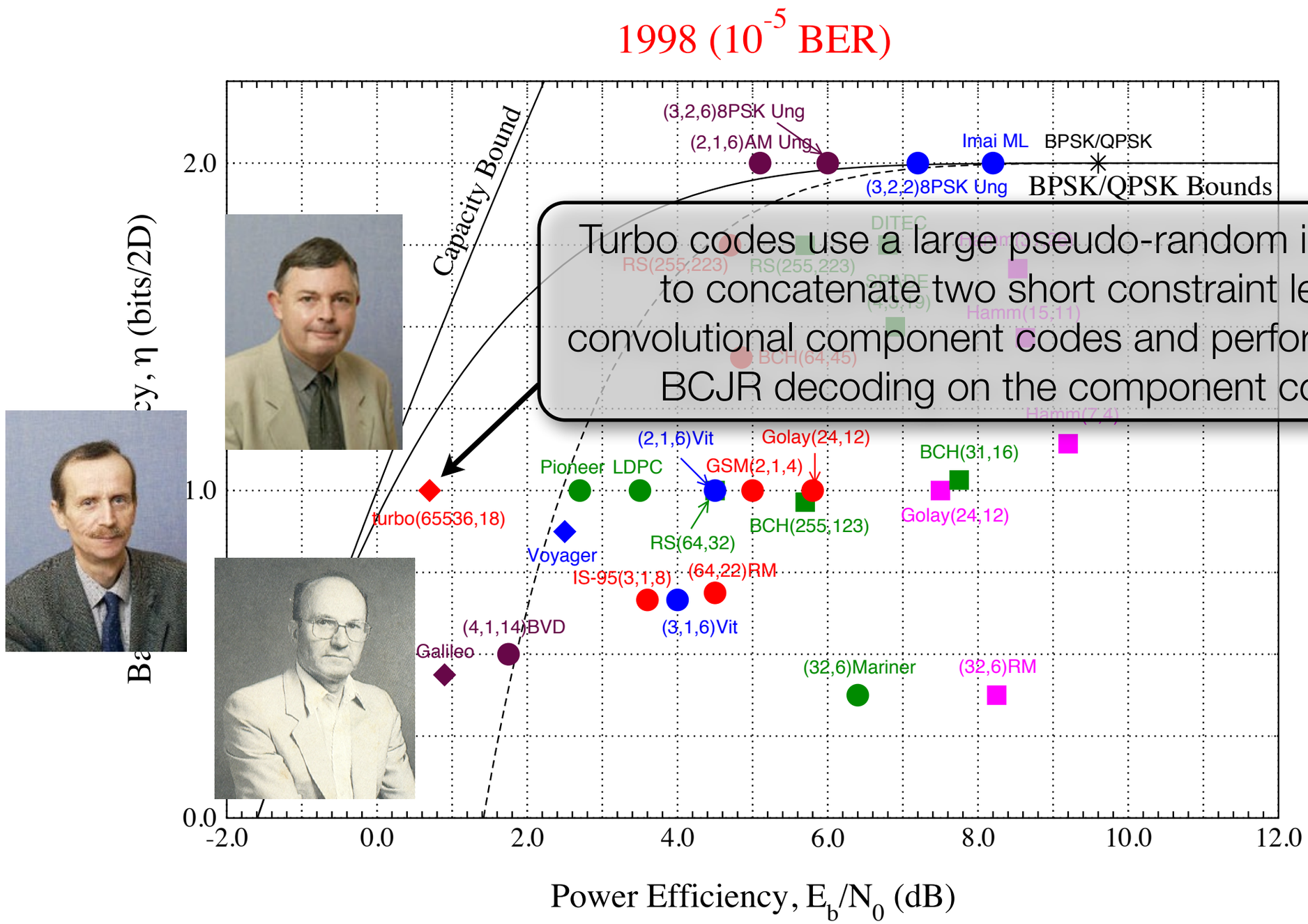
The Fifth Day



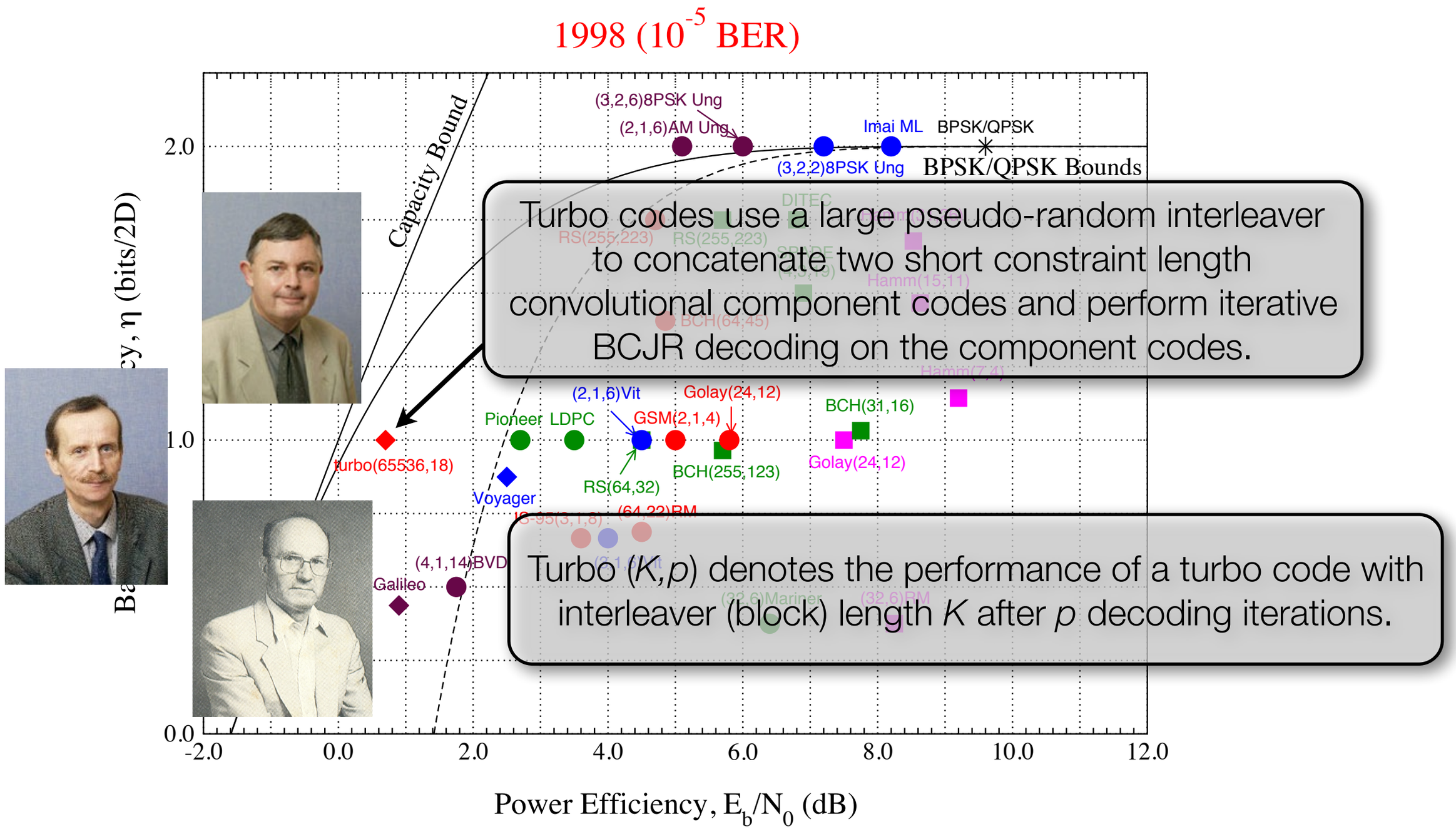
The Fifth Day



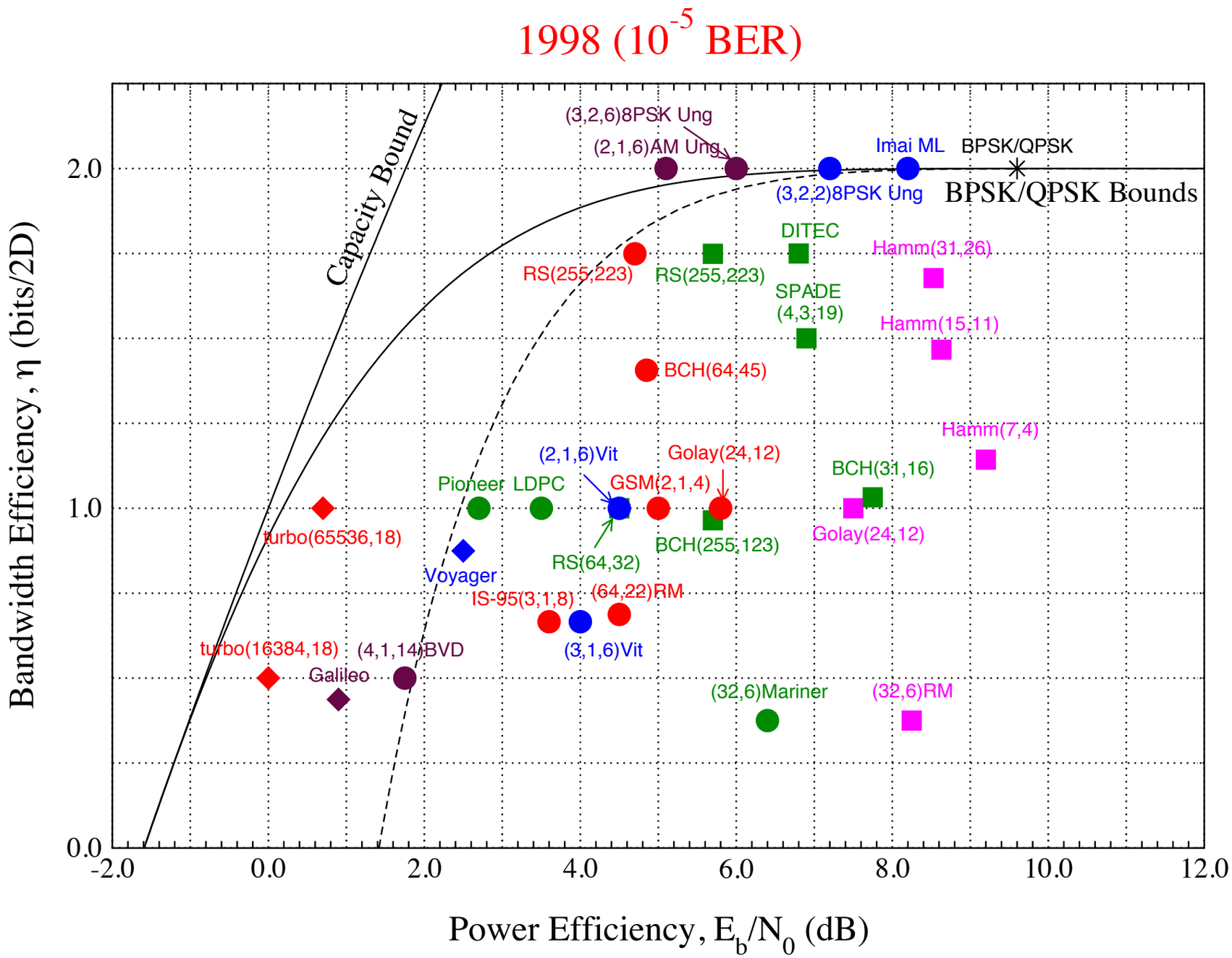
The Fifth Day



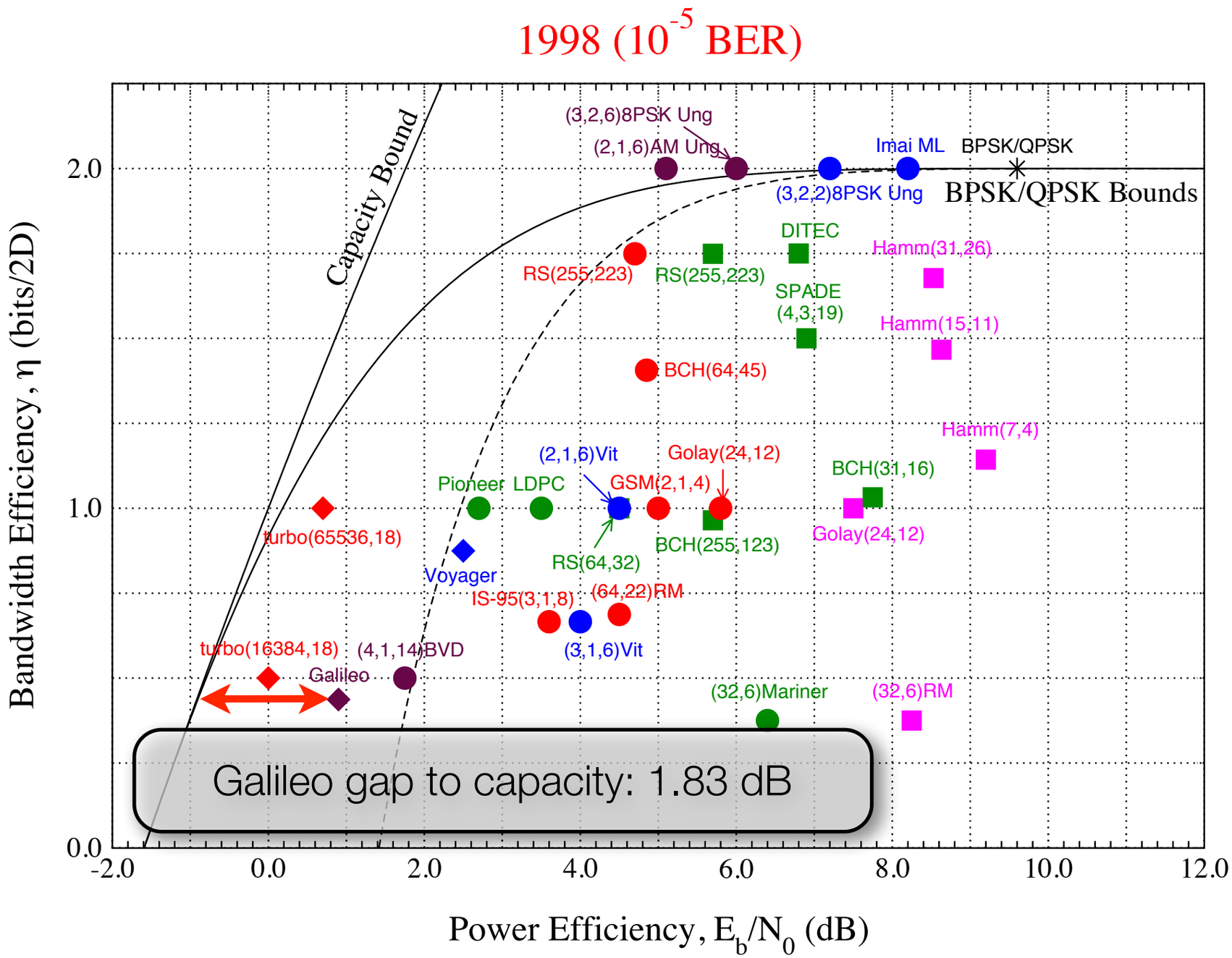
The Fifth Day



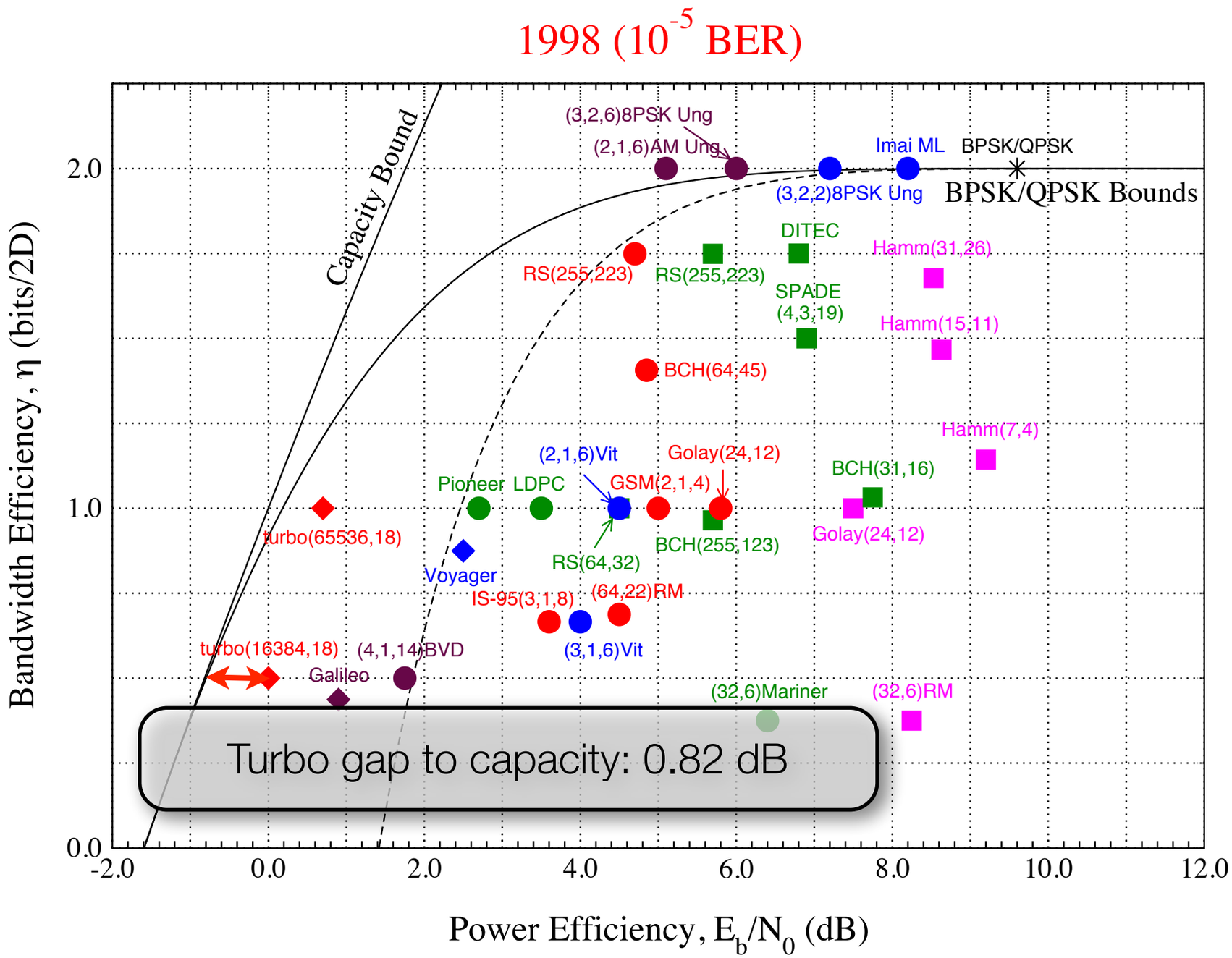
The Fifth Day



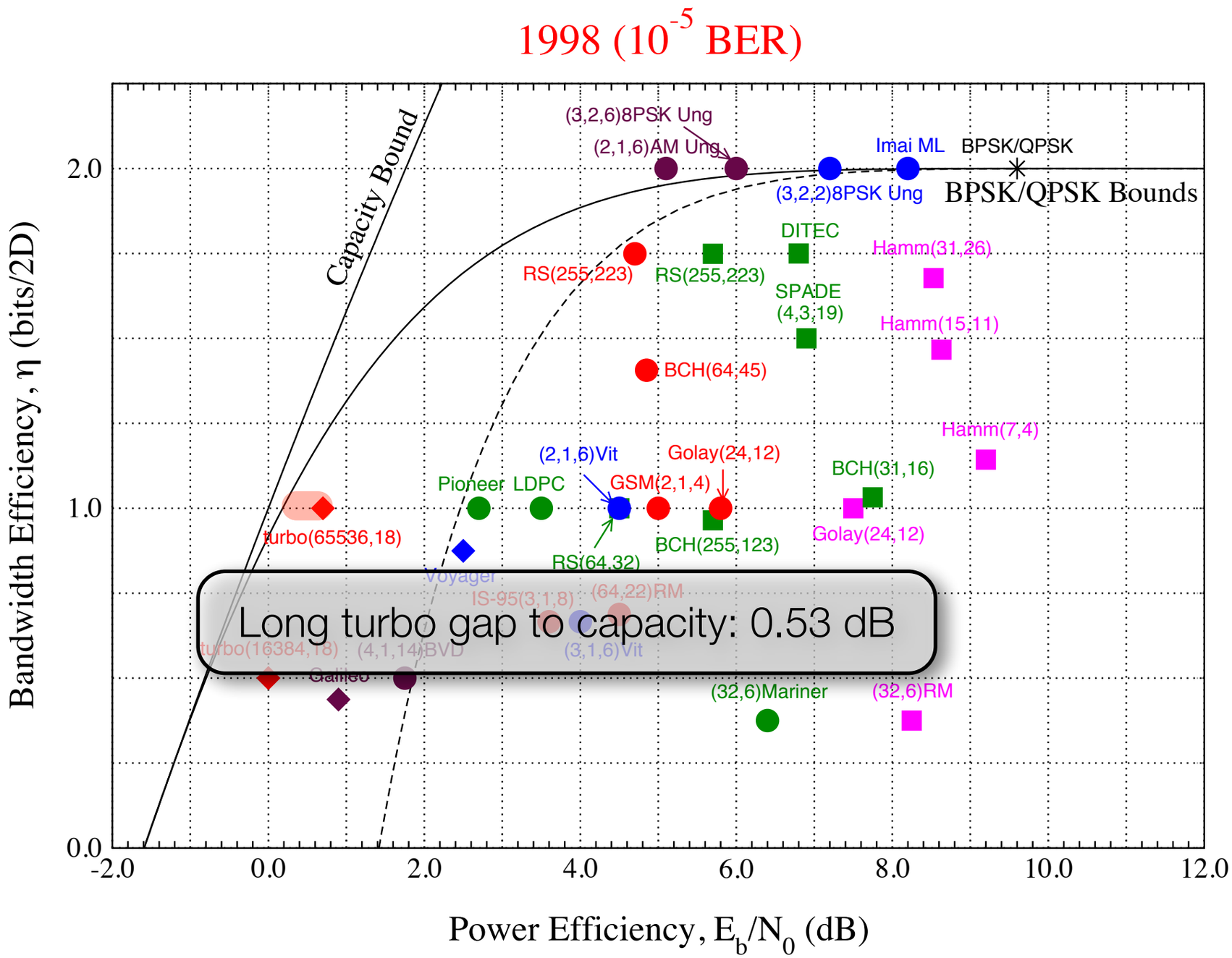
The Fifth Day



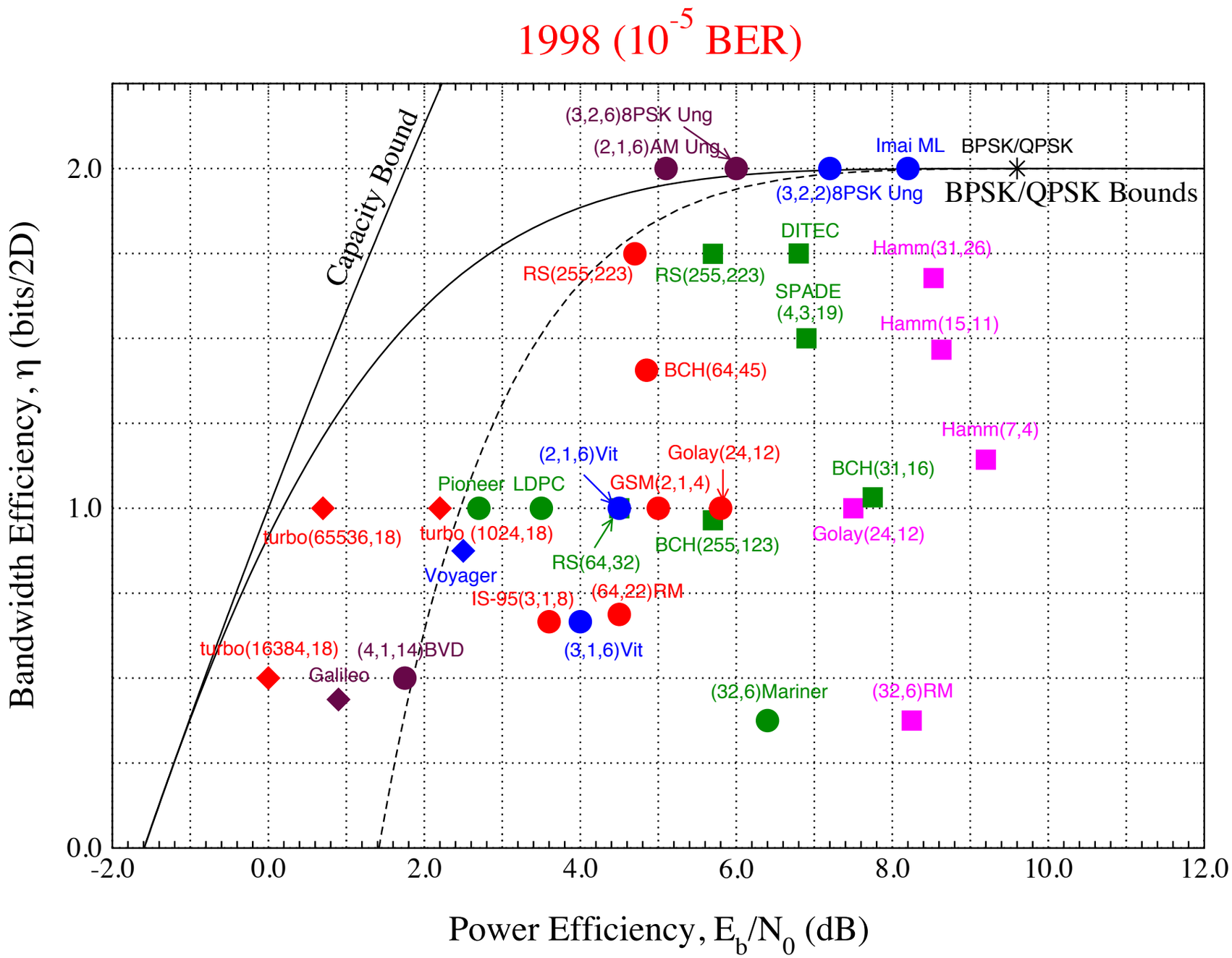
The Fifth Day



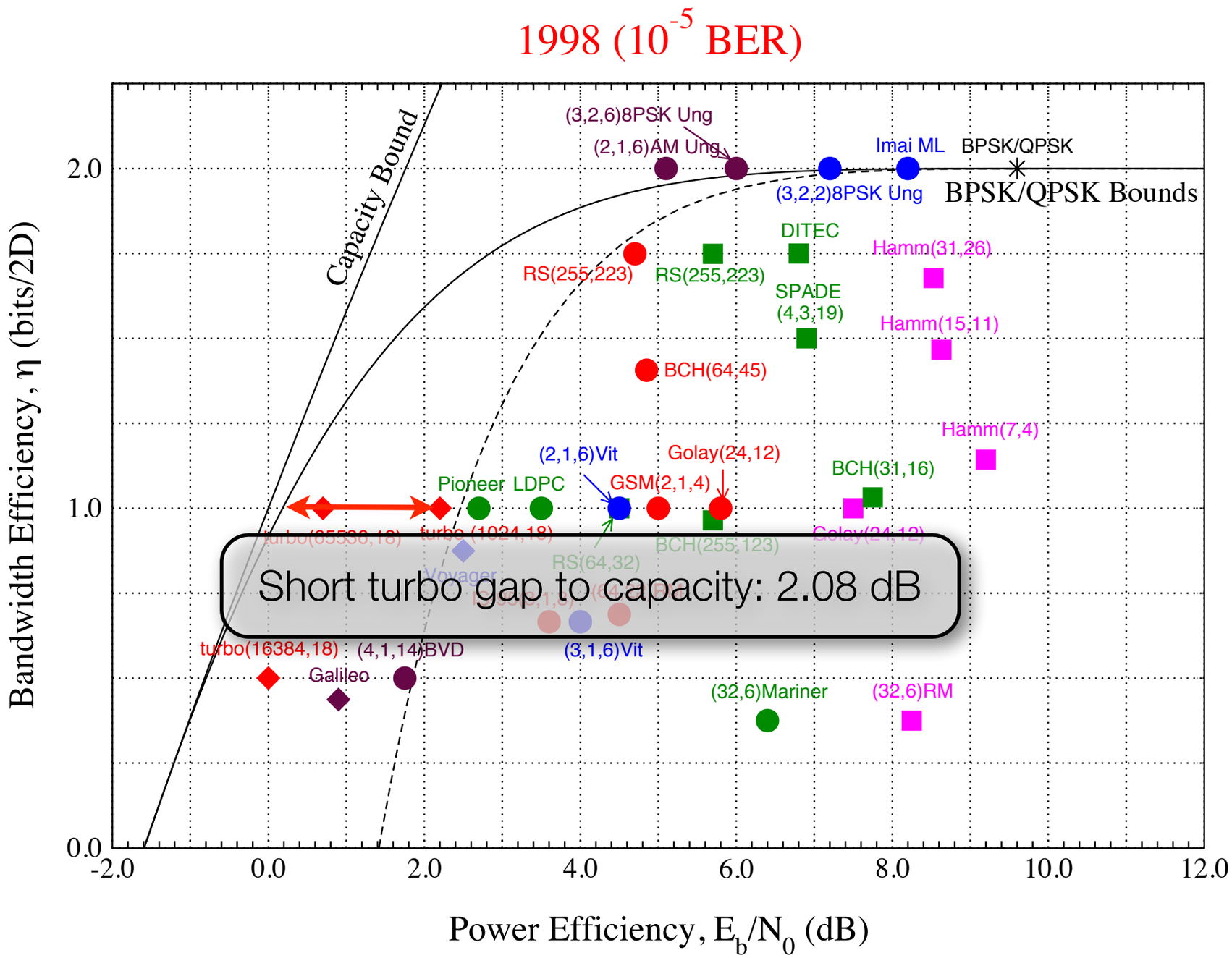
The Fifth Day



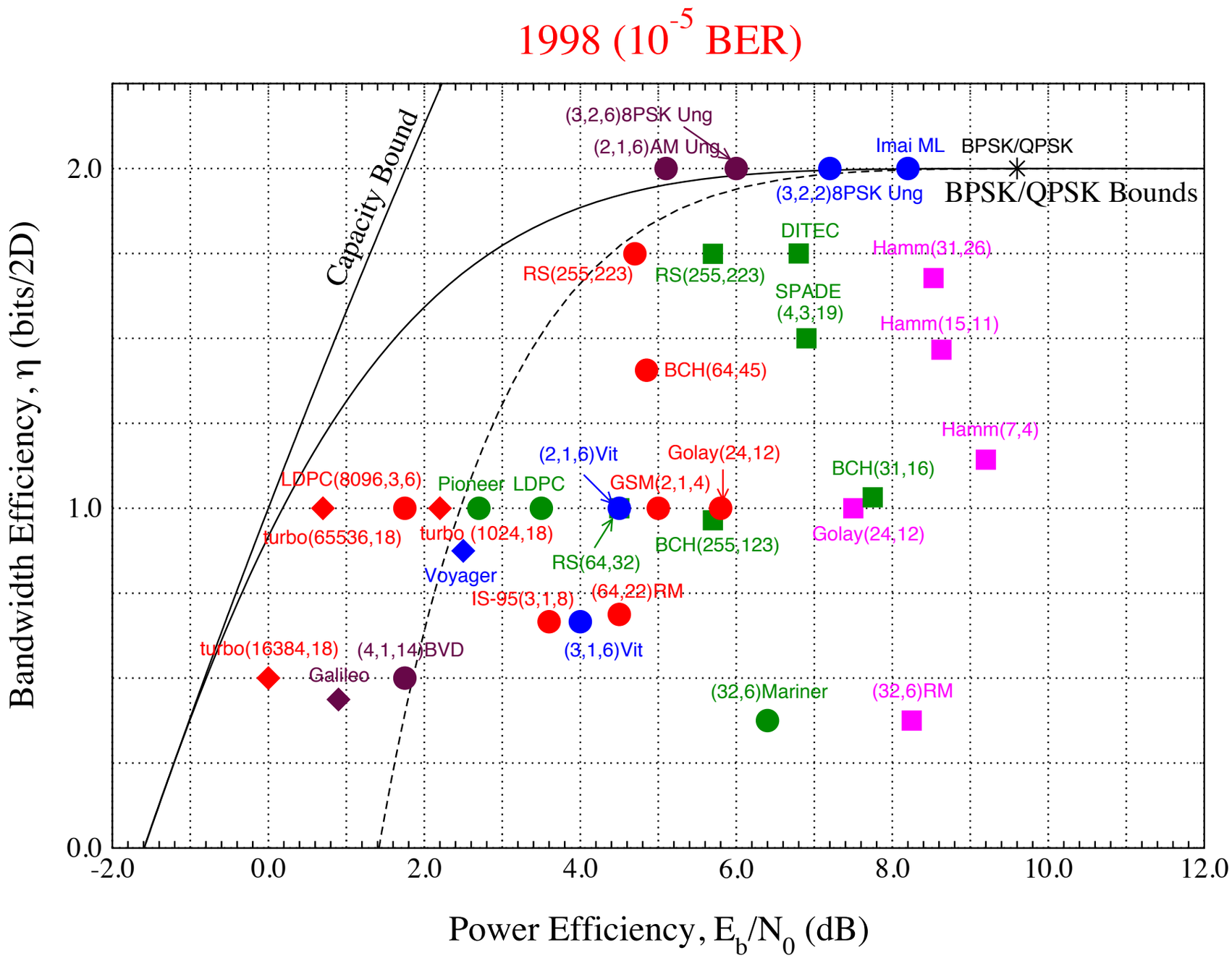
The Fifth Day



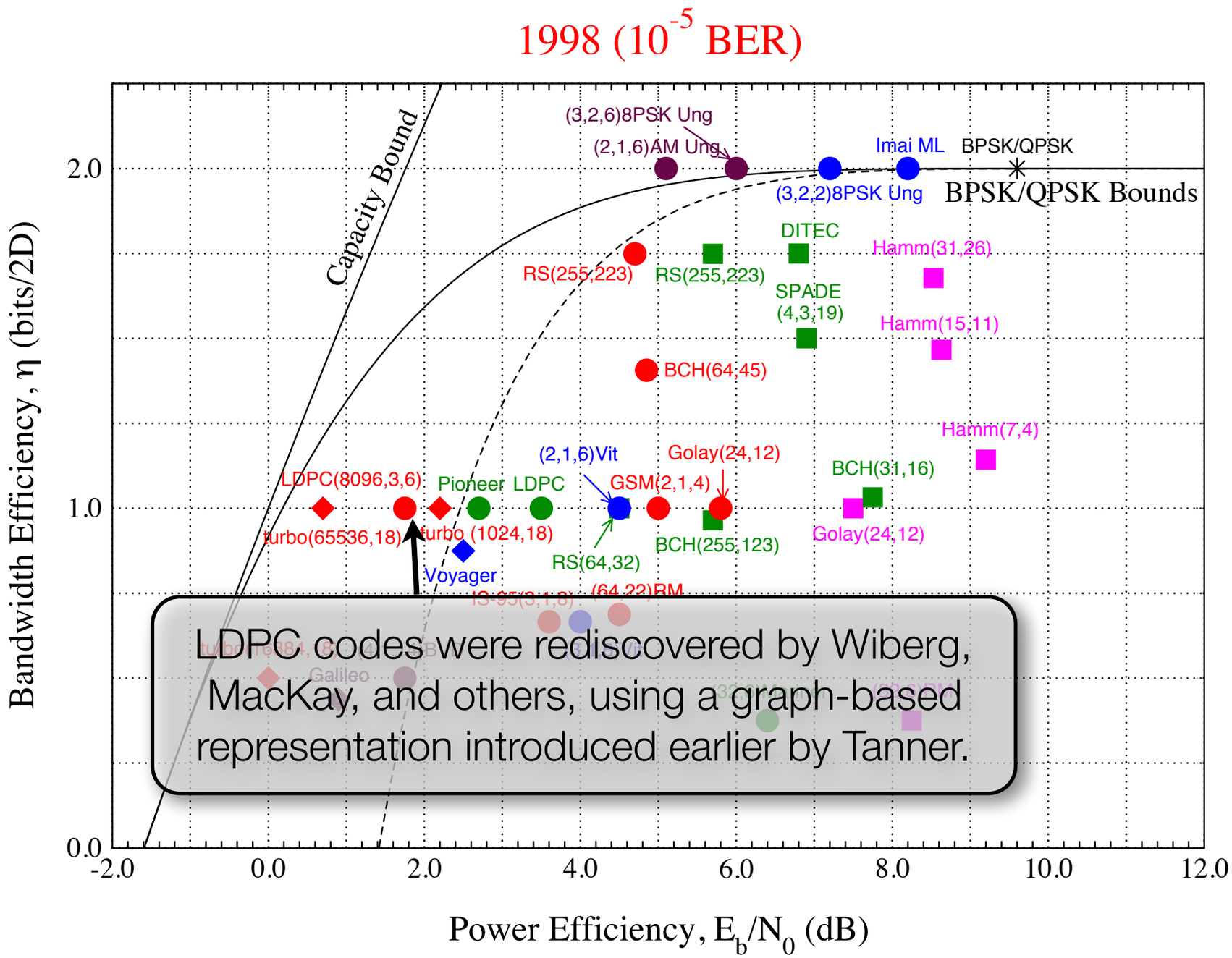
The Fifth Day



The Fifth Day

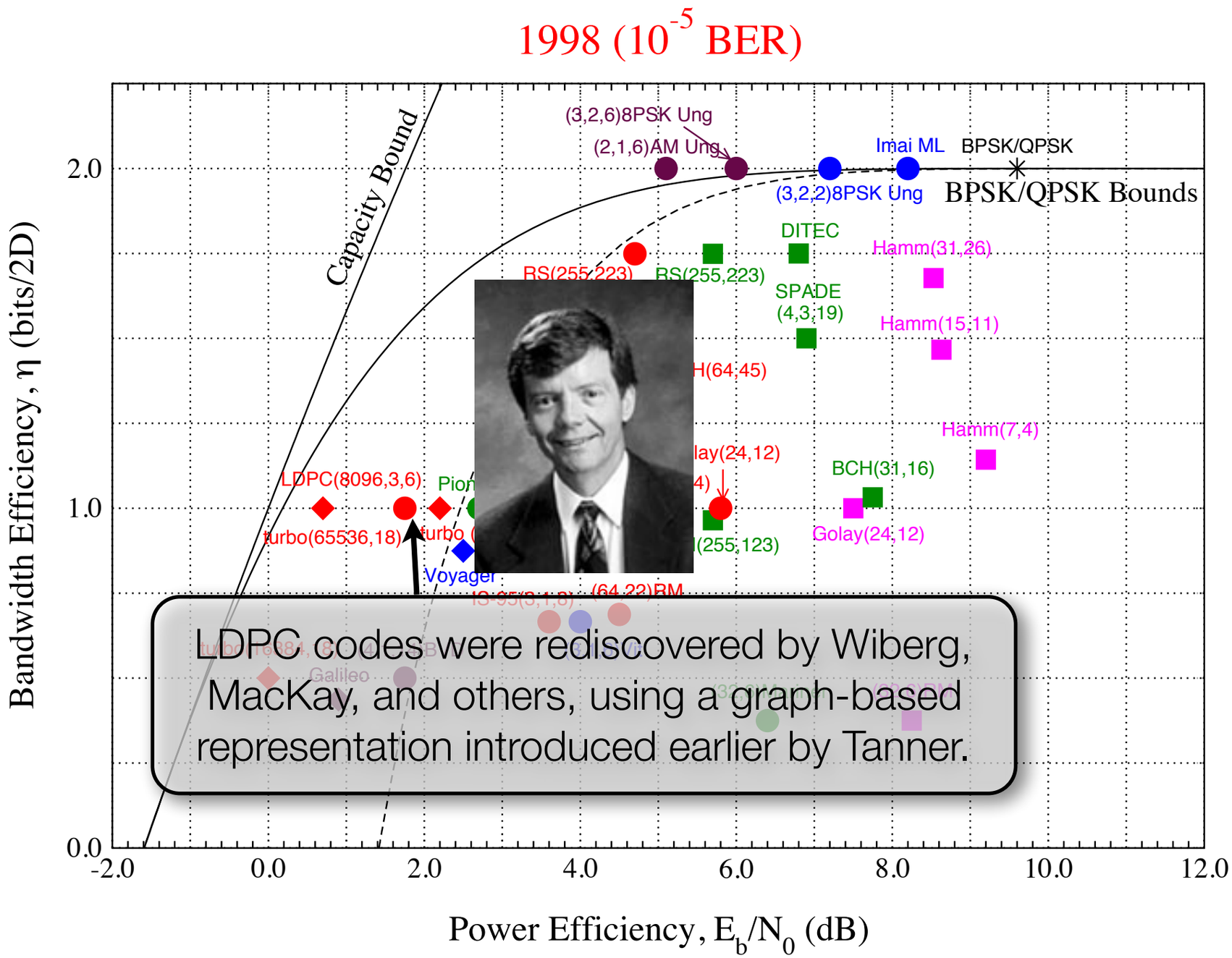


The Fifth Day



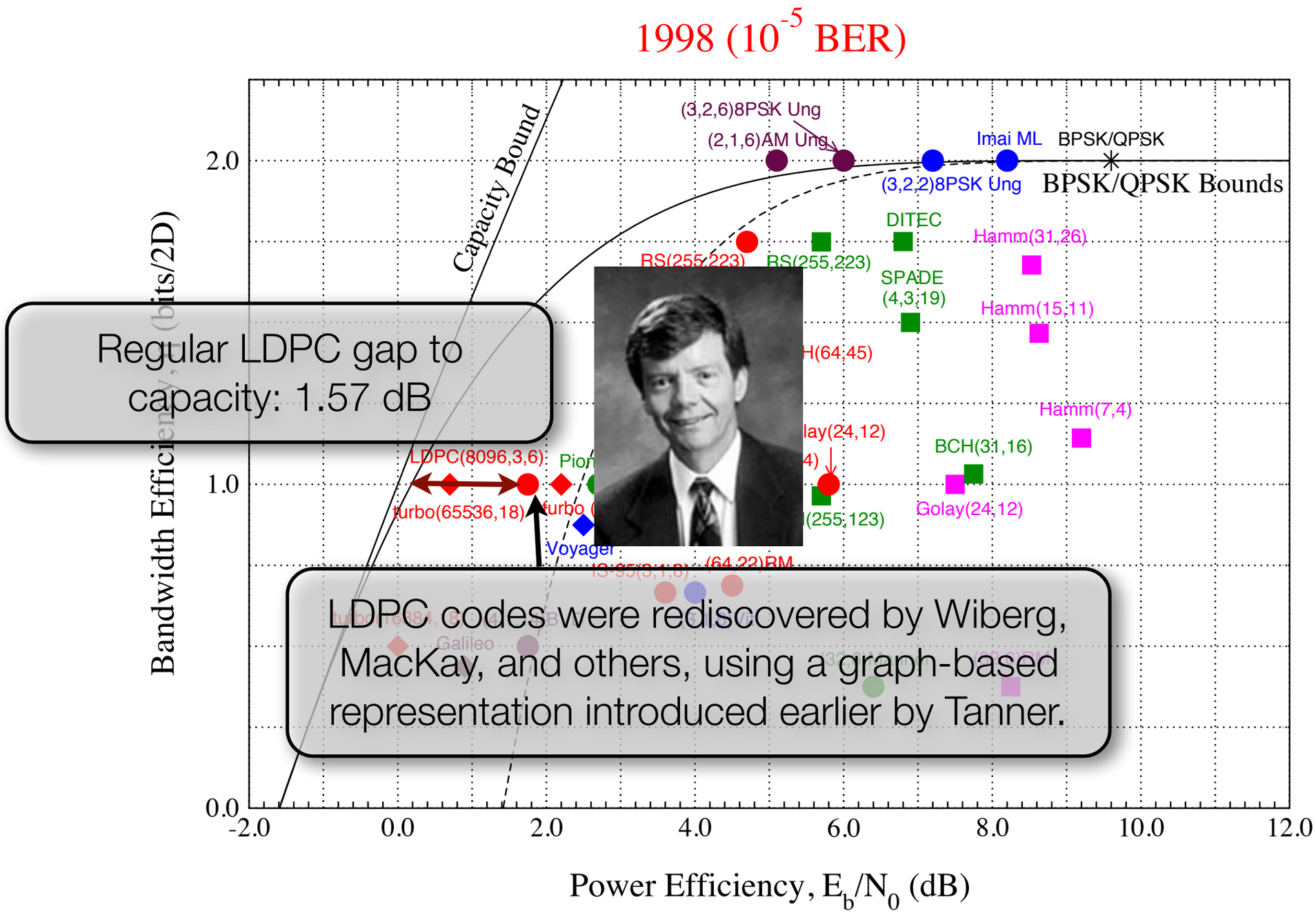
LDPC codes were rediscovered by Wiberg, MacKay, and others, using a graph-based representation introduced earlier by Tanner.

The Fifth Day



LDPC codes were rediscovered by Wiberg, MacKay, and others, using a graph-based representation introduced earlier by Tanner.

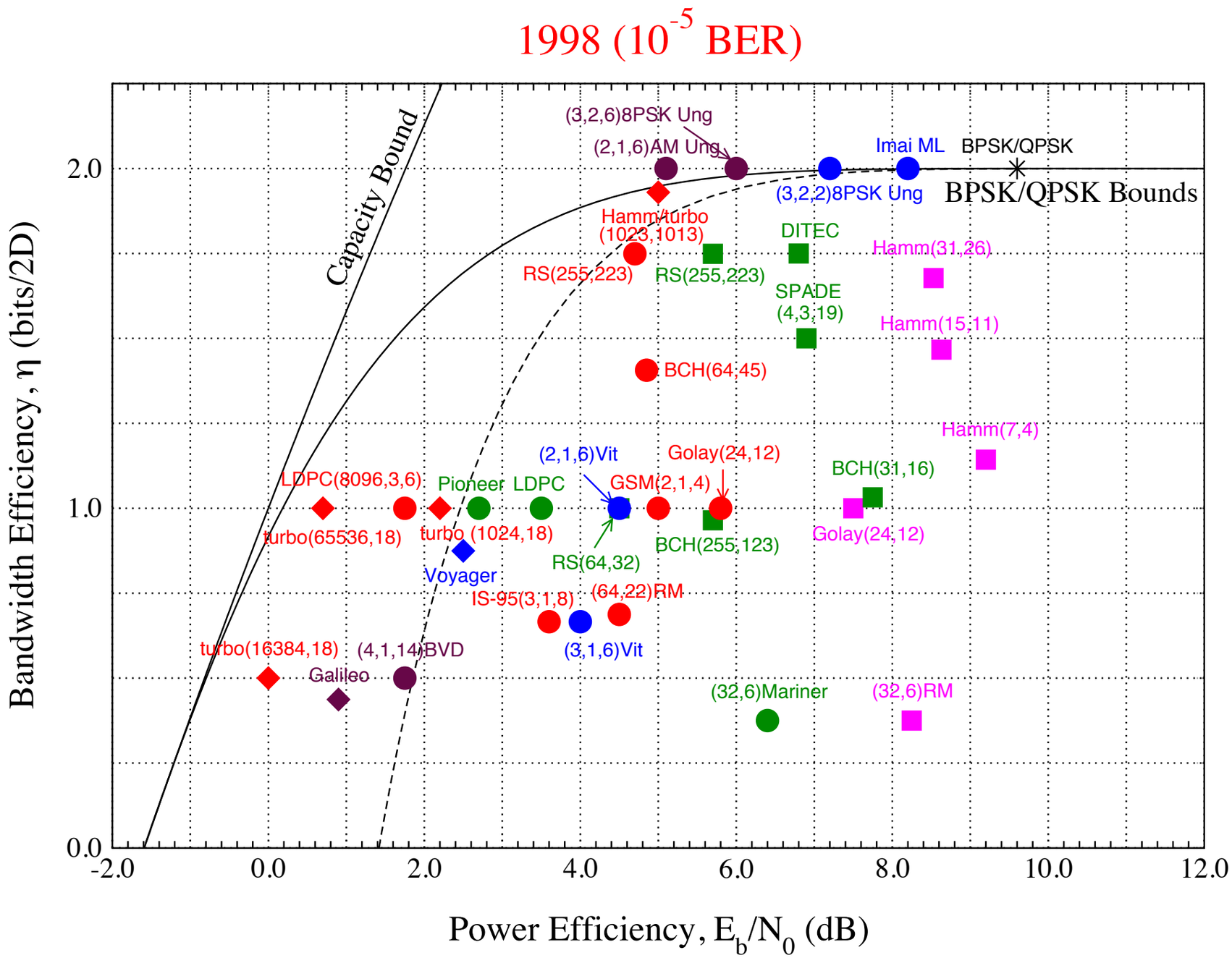
The Fifth Day



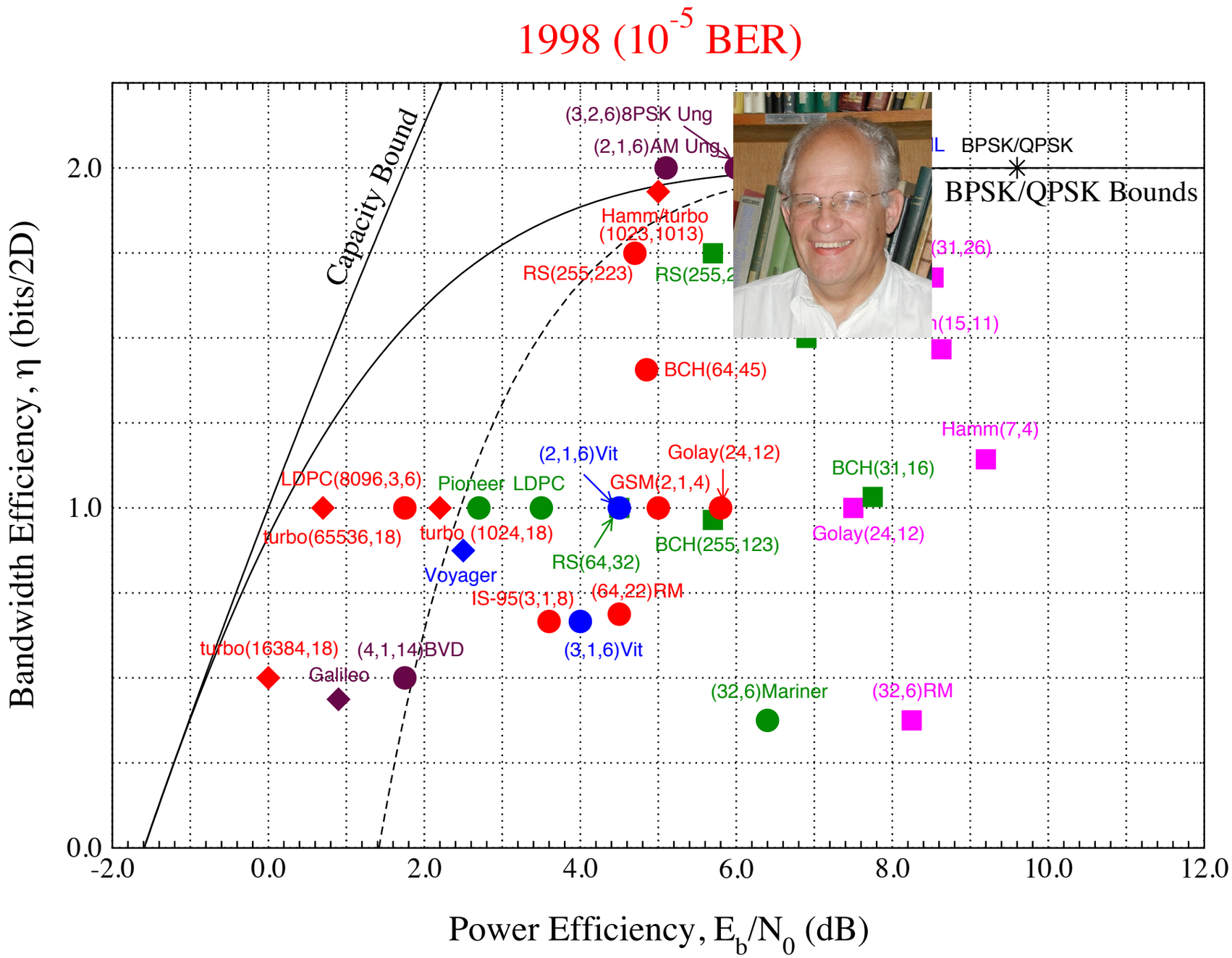
Regular LDPC gap to capacity: 1.57 dB

LDPC codes were rediscovered by Wiberg, MacKay, and others, using a graph-based representation introduced earlier by Tanner.

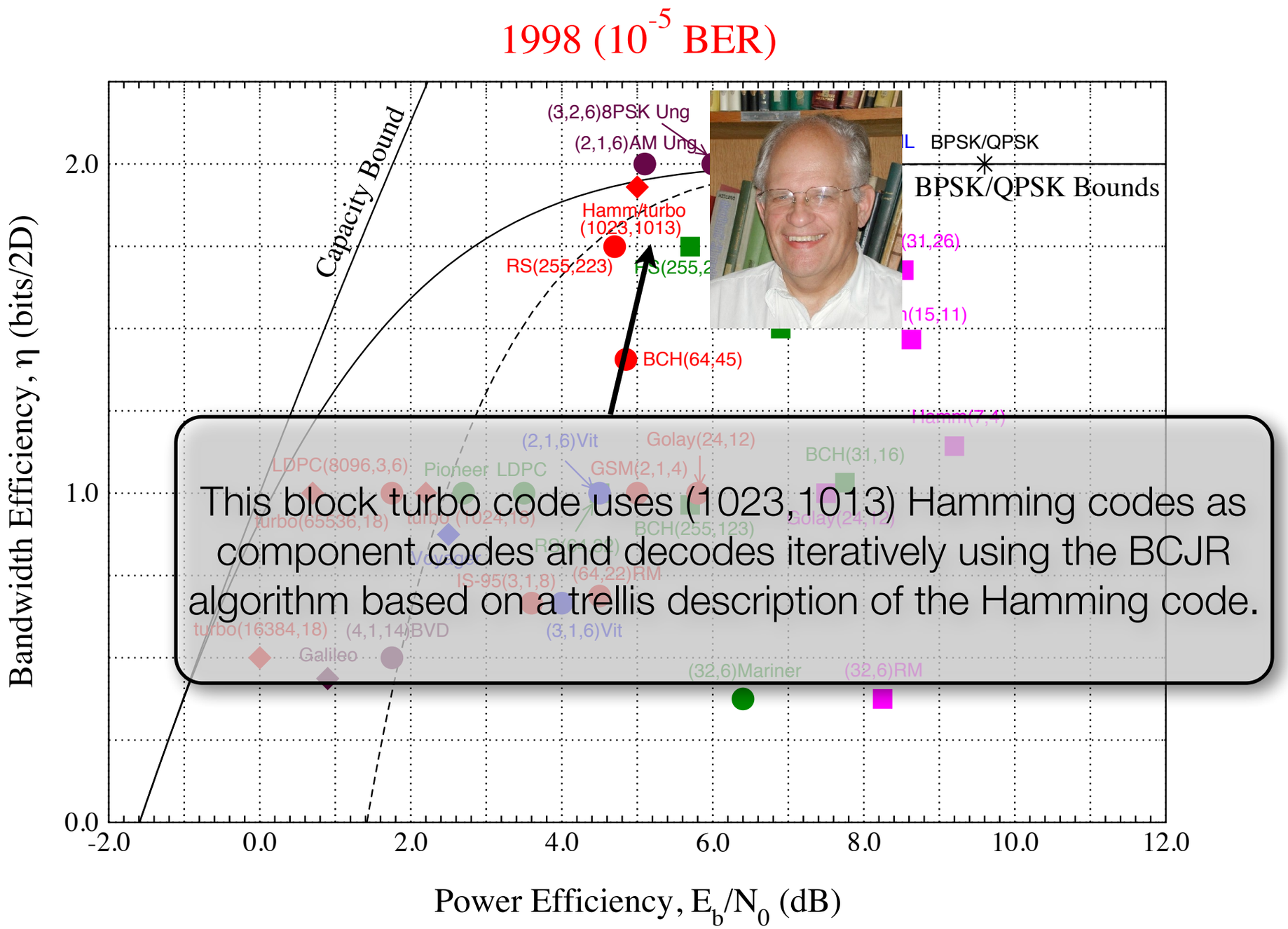
The Fifth Day



The Fifth Day

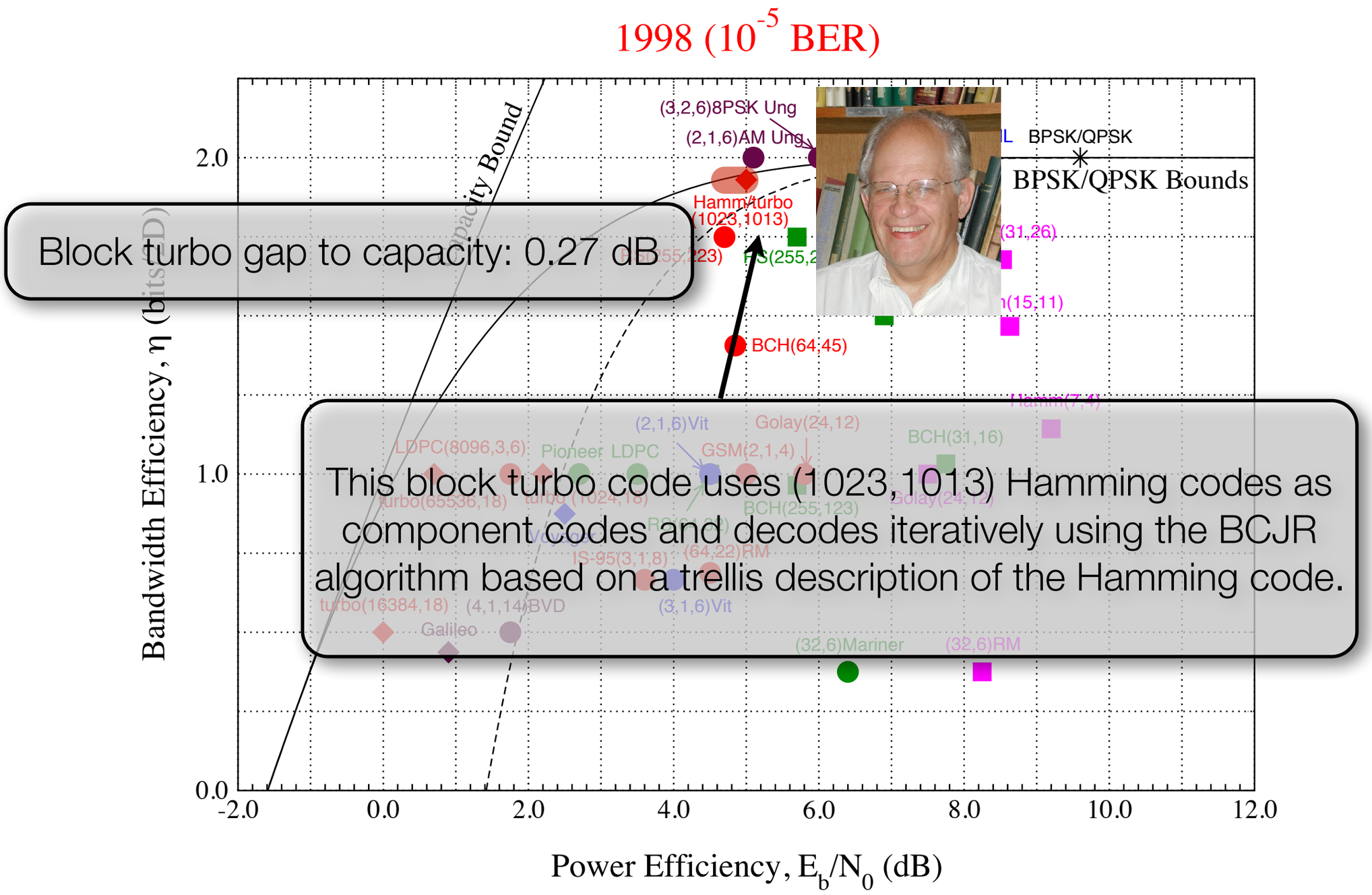


The Fifth Day



This block turbo code uses (1023,1013) Hamming codes as component codes and decodes iteratively using the BCJR algorithm based on a trellis description of the Hamming code.

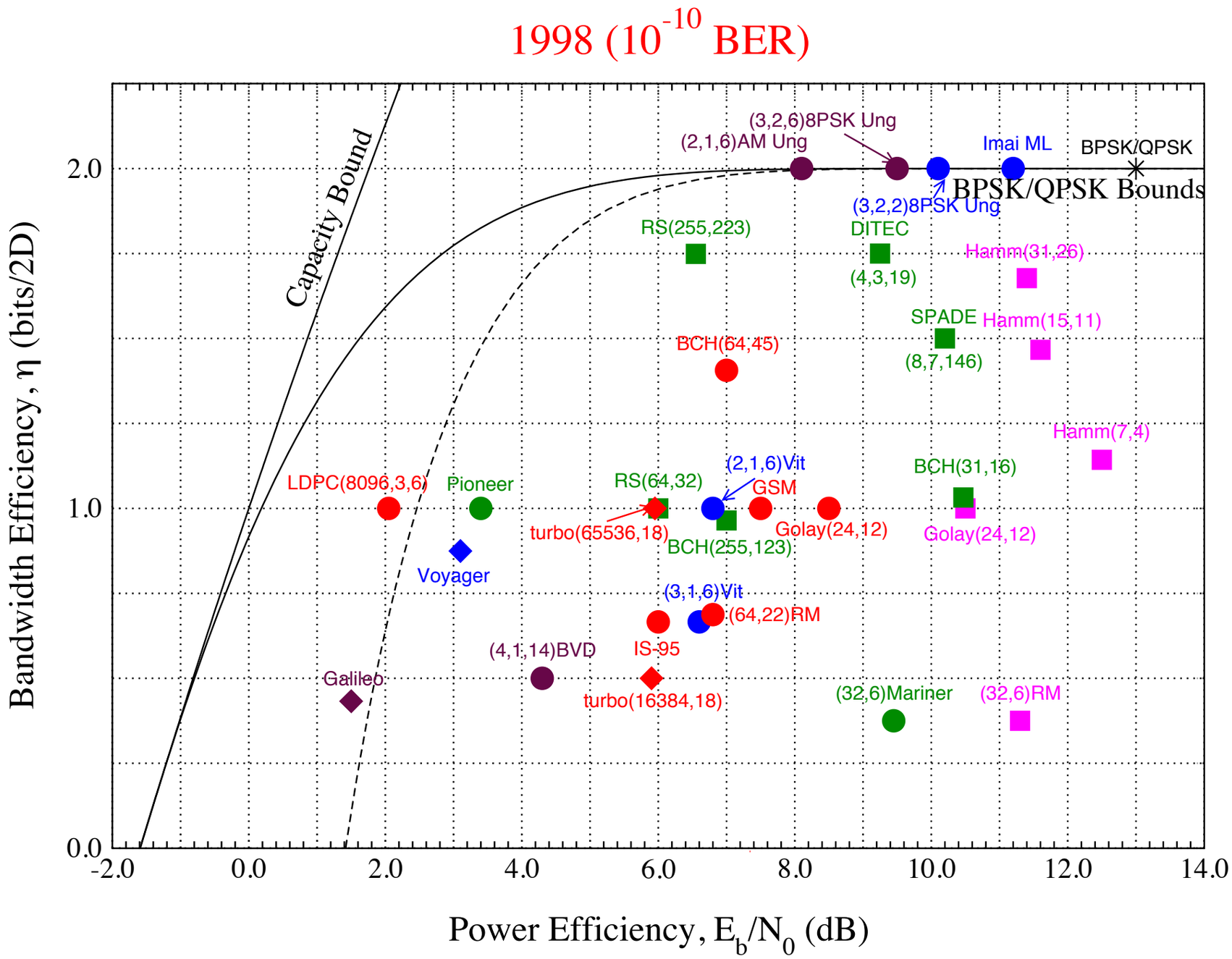
The Fifth Day



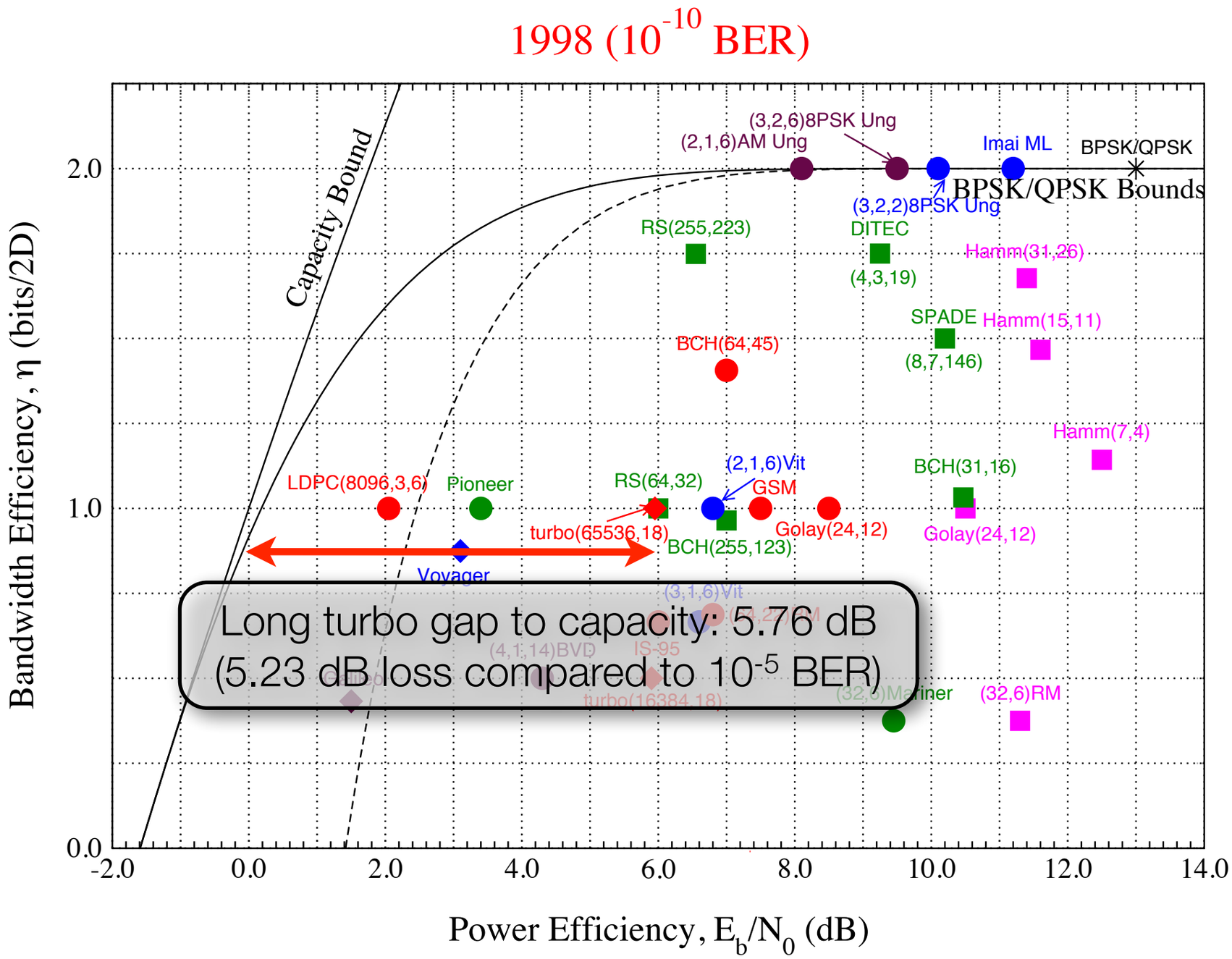
Block turbo gap to capacity: 0.27 dB

This block turbo code uses (1023,1013) Hamming codes as component codes and decodes iteratively using the BCJR algorithm based on a trellis description of the Hamming code.

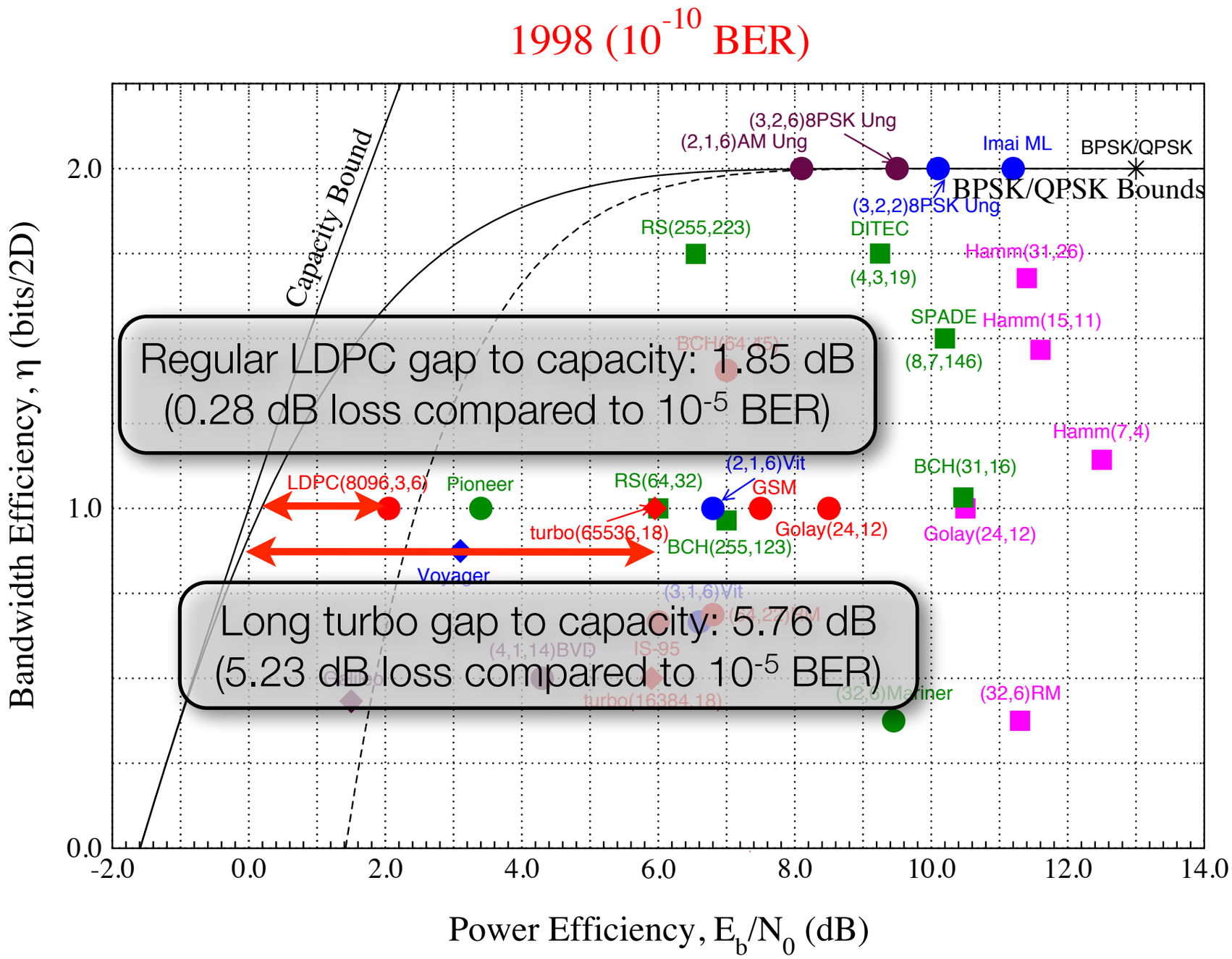
The Fifth Day



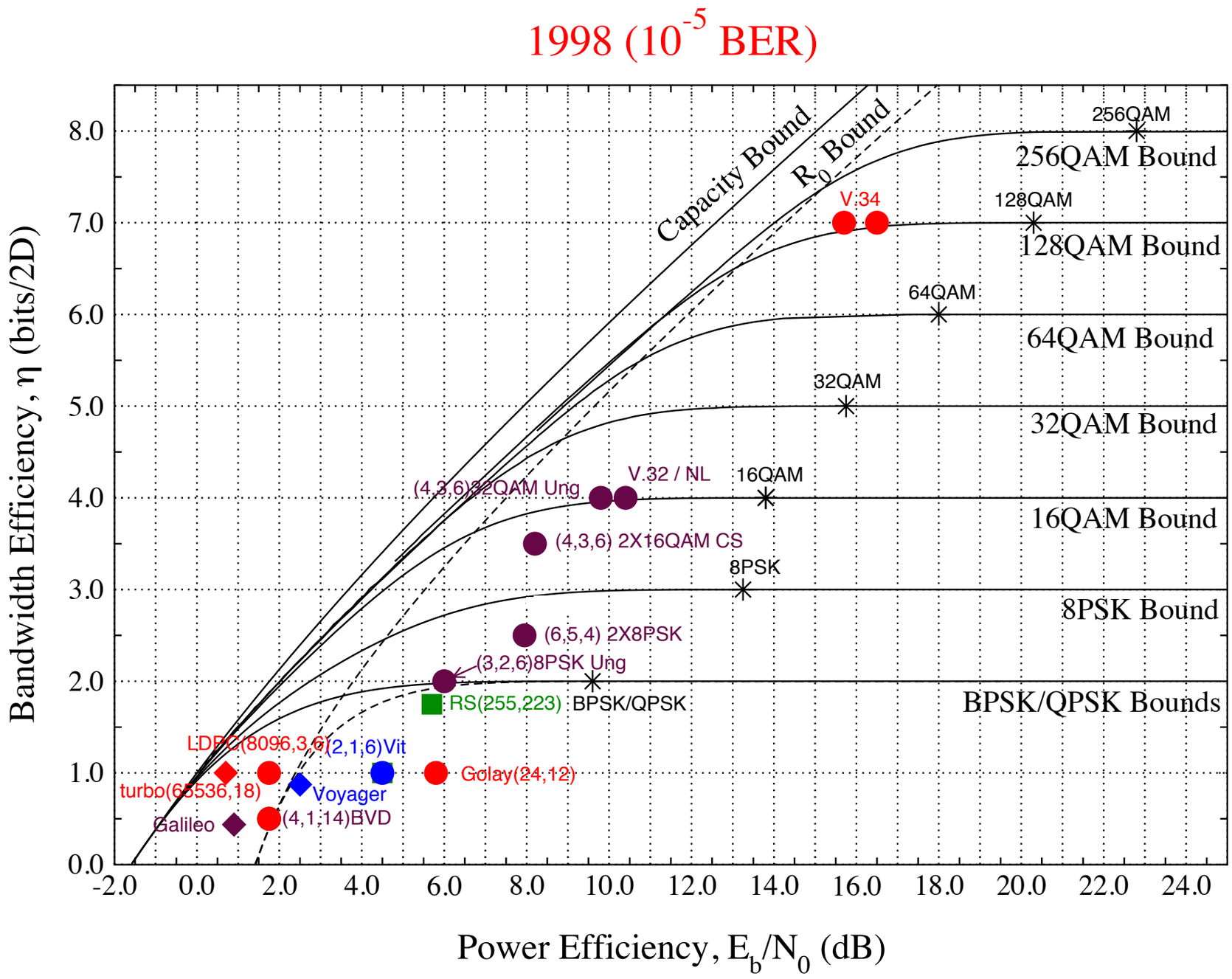
The Fifth Day



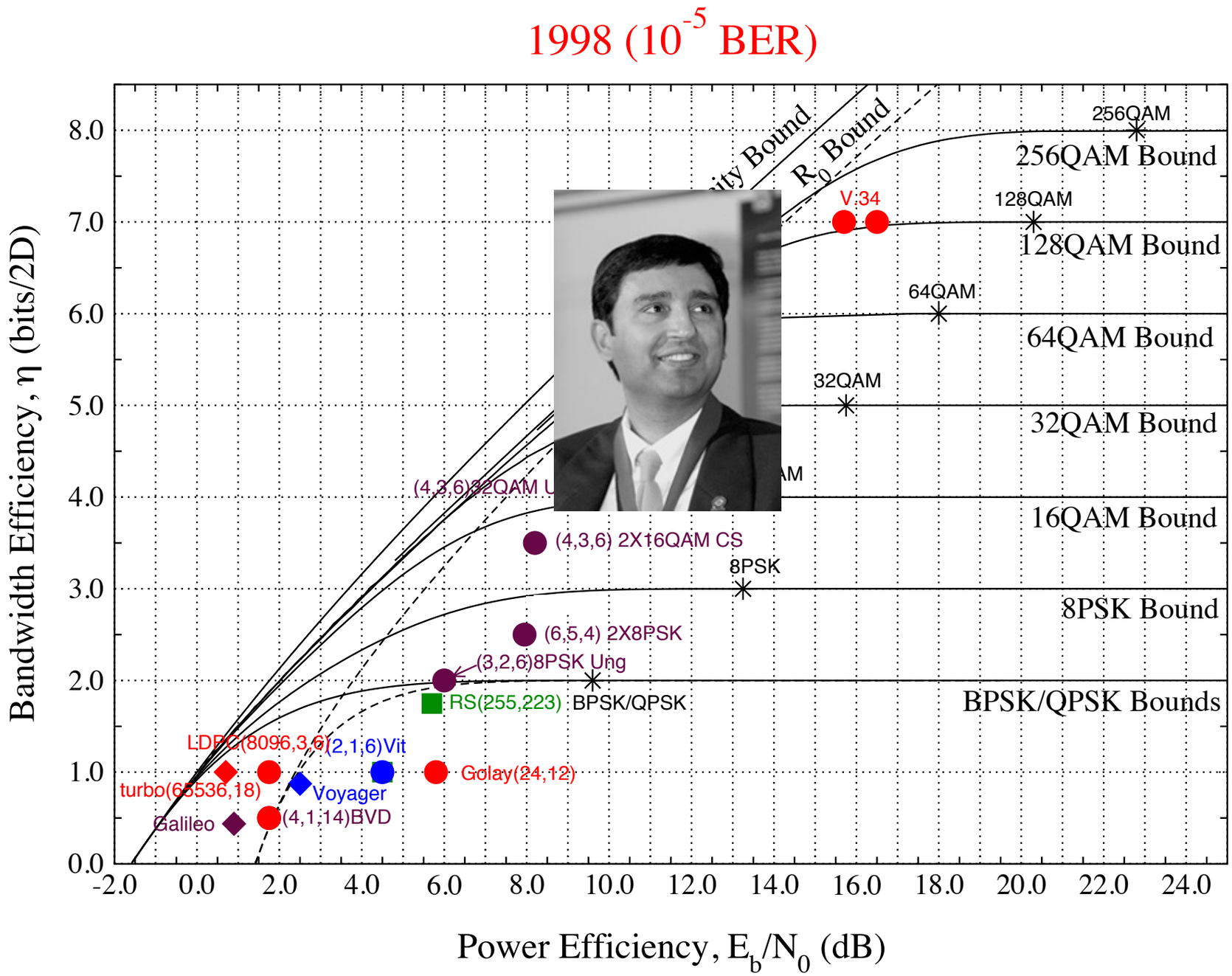
The Fifth Day



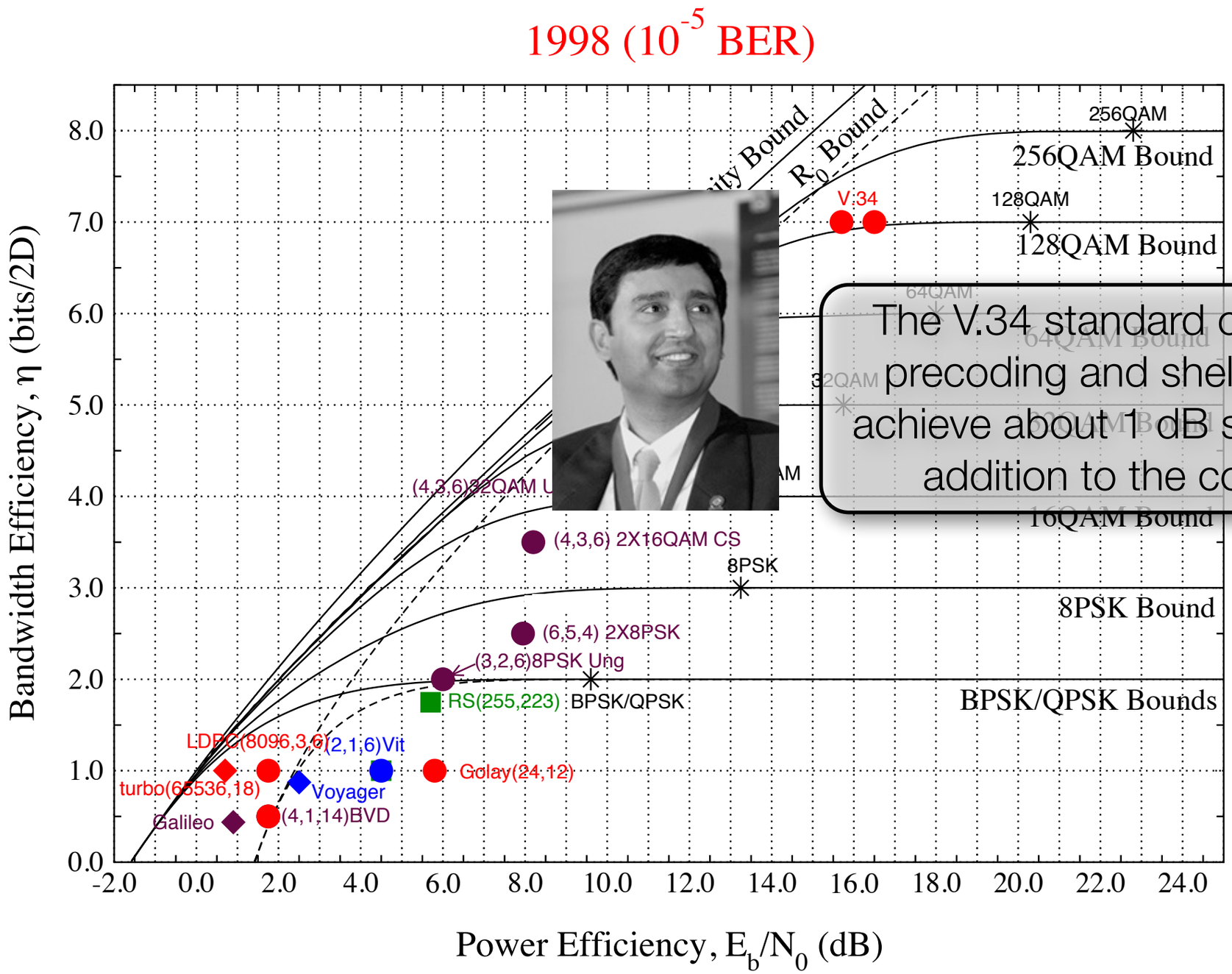
The Fifth Day



The Fifth Day

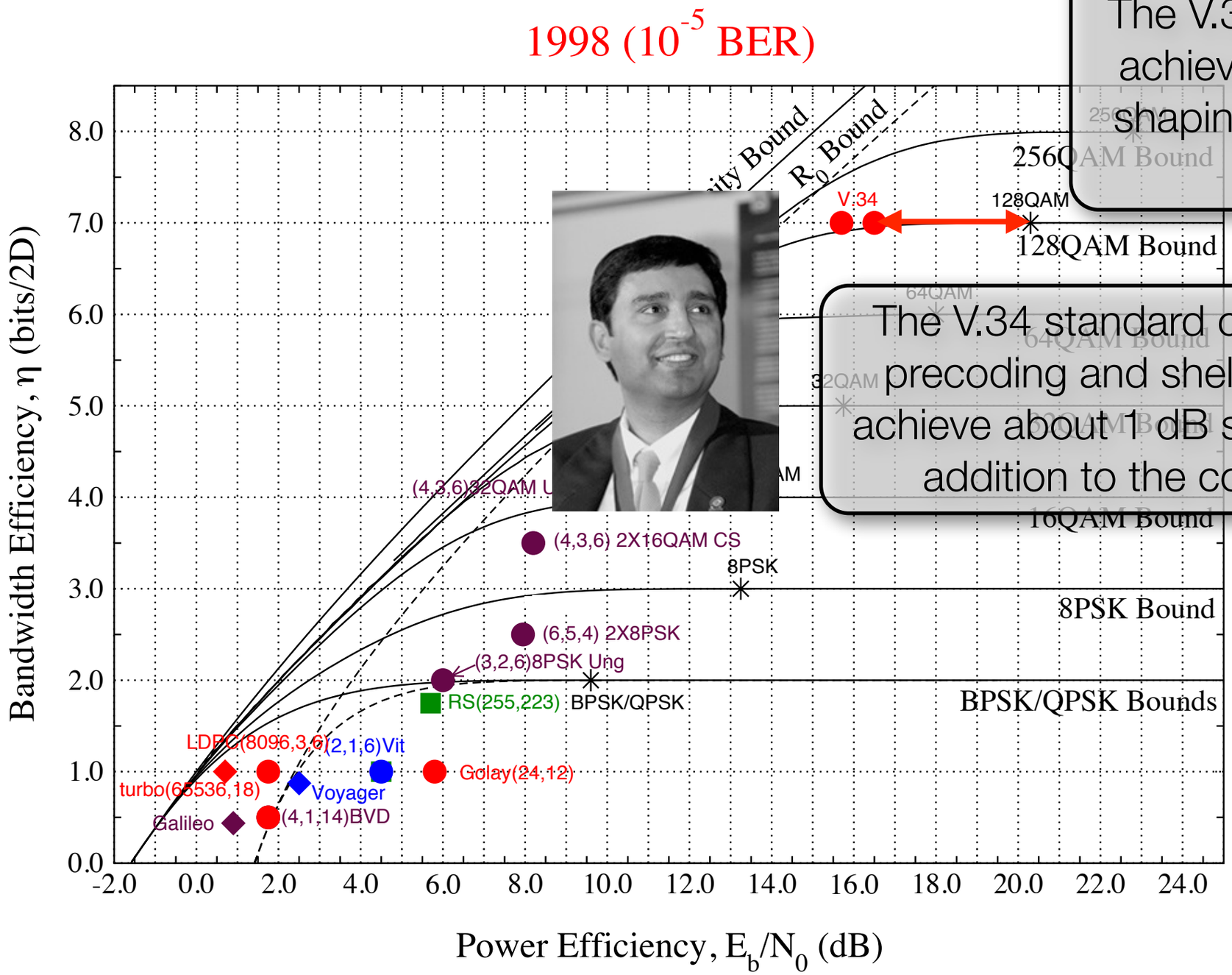


The Fifth Day



The V.34 standard codes employ precoding and shell mapping to achieve about 1 dB shaping gain in addition to the coding gain.

The Fifth Day



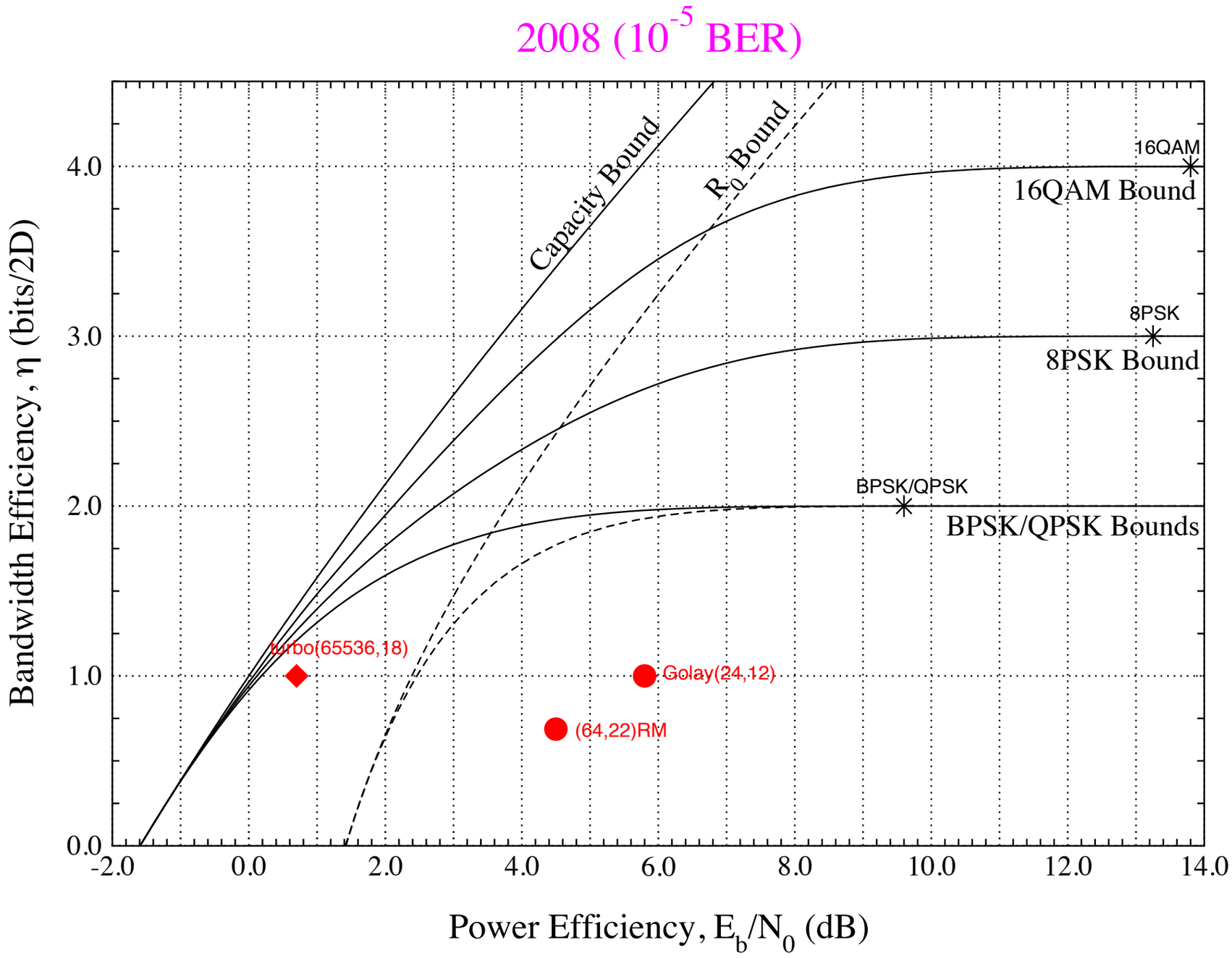
The V.34 standard code achieves a coding plus shaping gain of 3.7 dB.

The V.34 standard codes employ precoding and shell mapping to achieve about 1 dB shaping gain in addition to the coding gain.

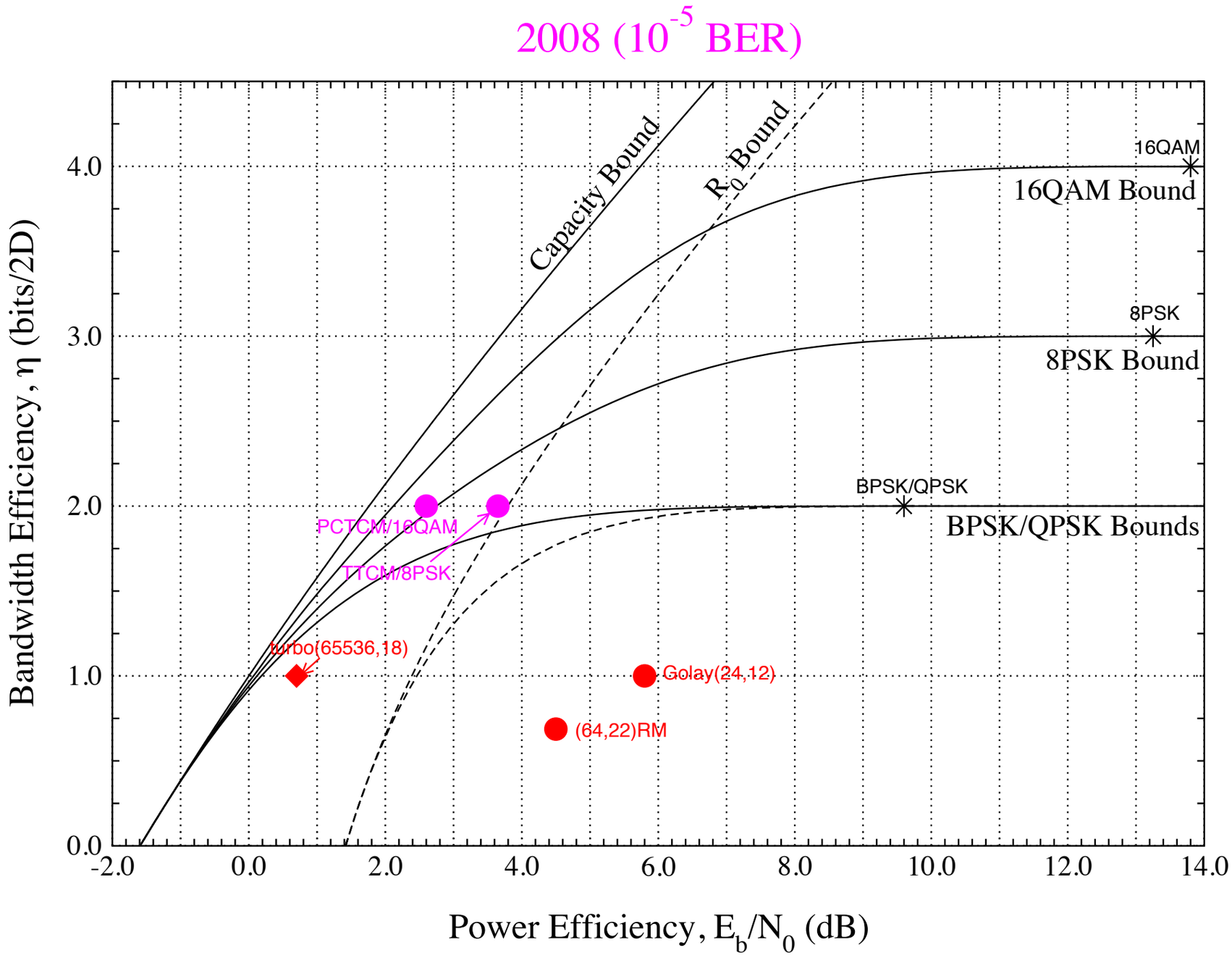
The Sixth Day

The Sixth Day

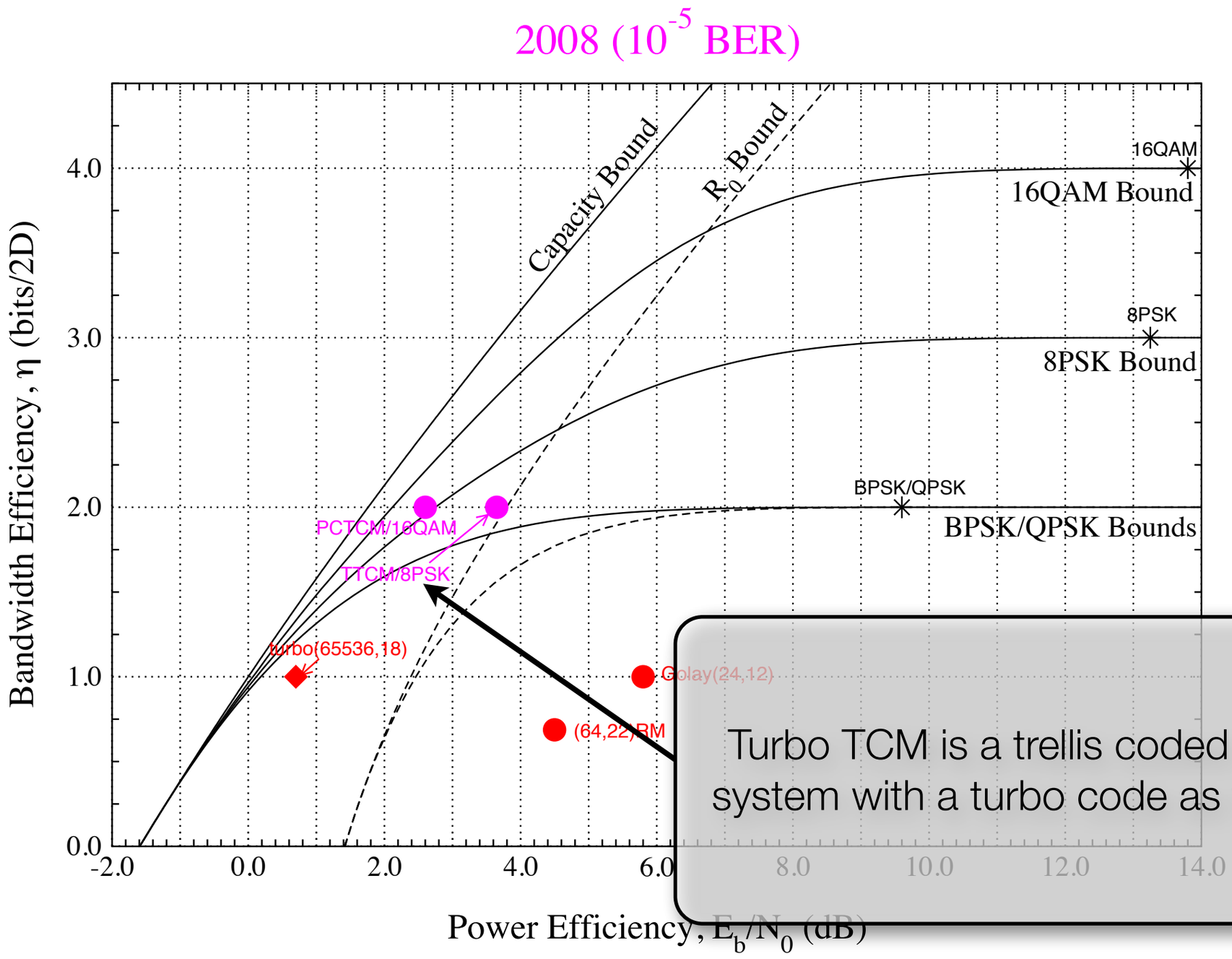
The Sixth Day



The Sixth Day

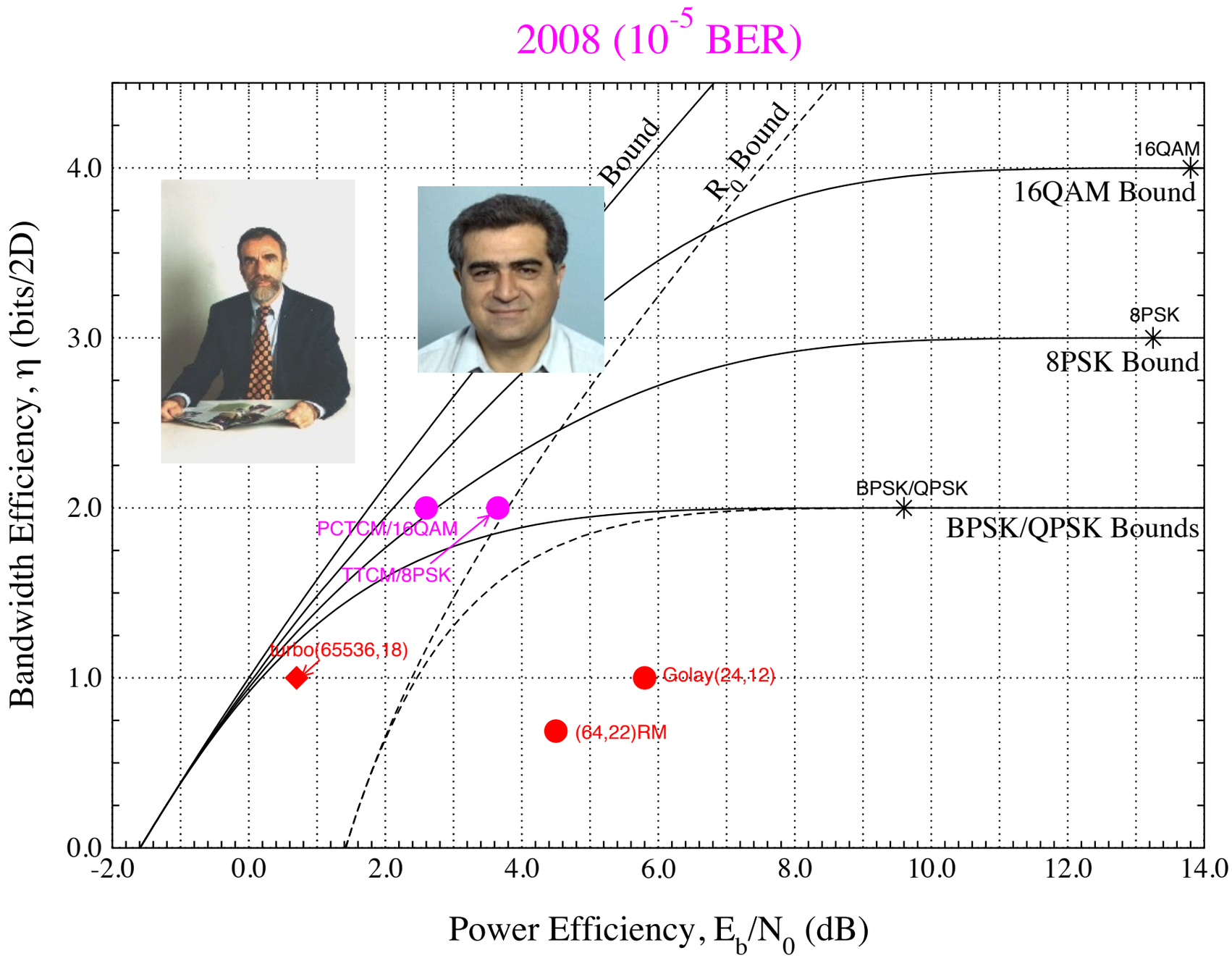


The Sixth Day

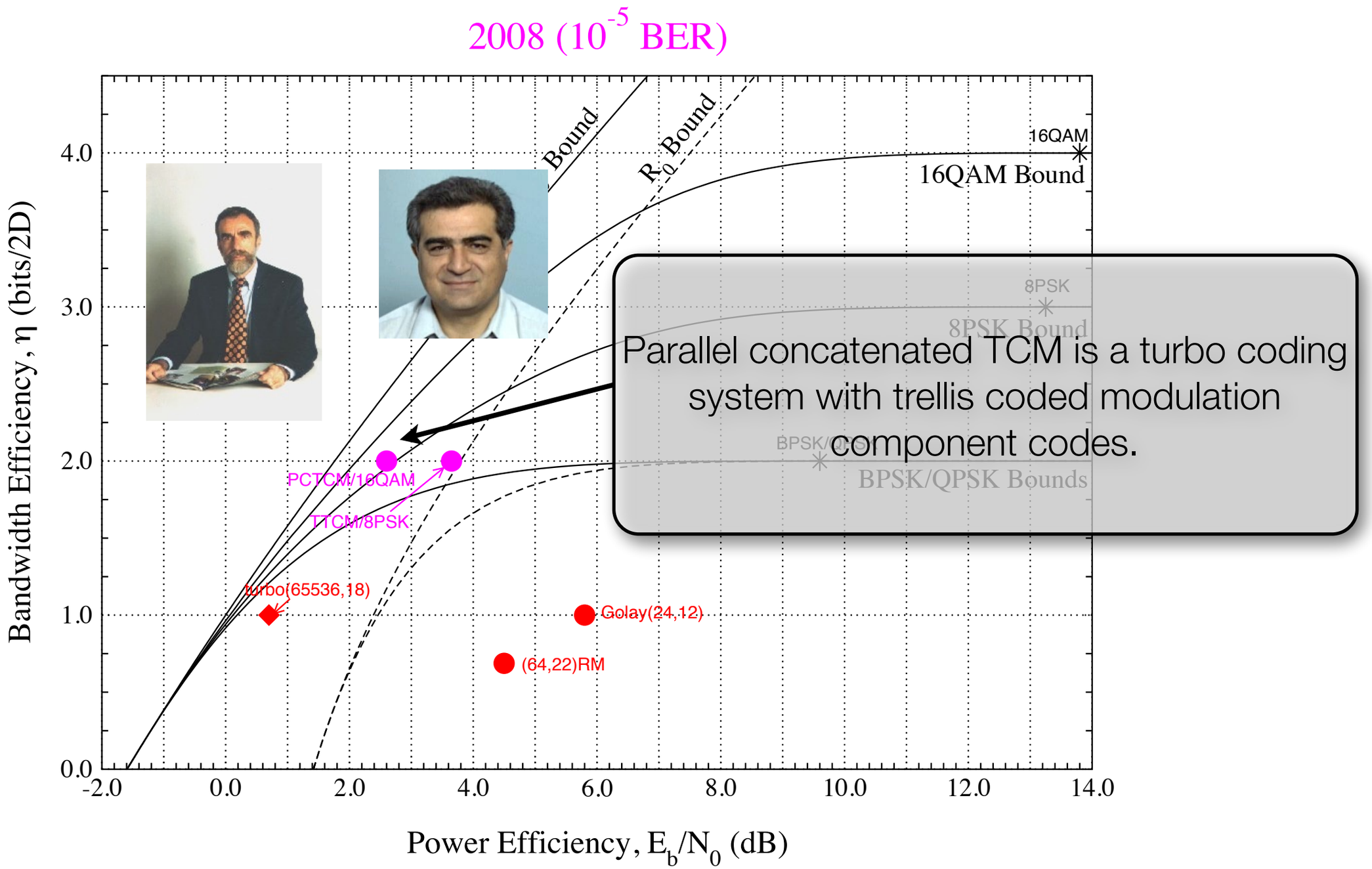


Turbo TCM is a trellis coded modulation system with a turbo code as the encoder.

The Sixth Day

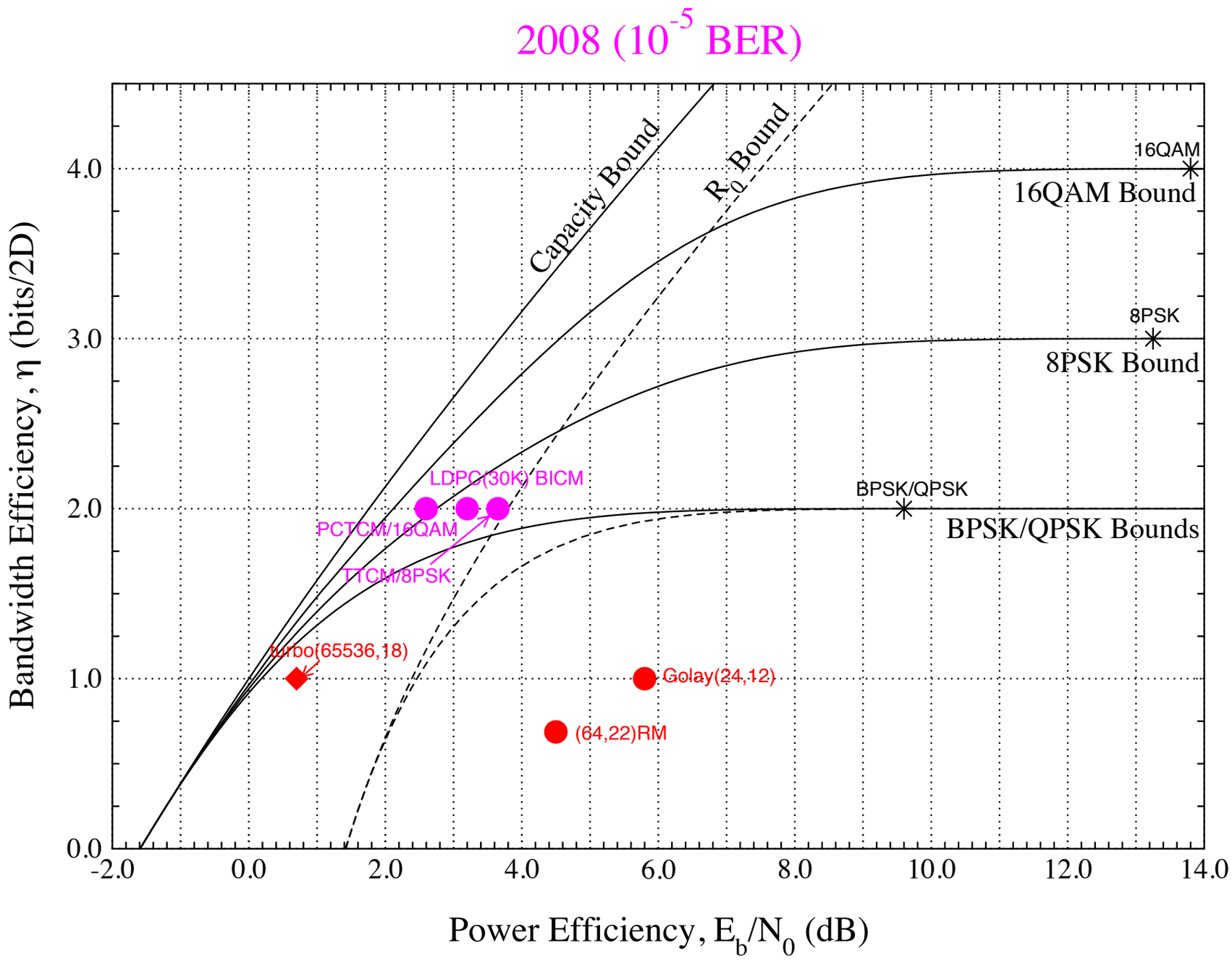


The Sixth Day

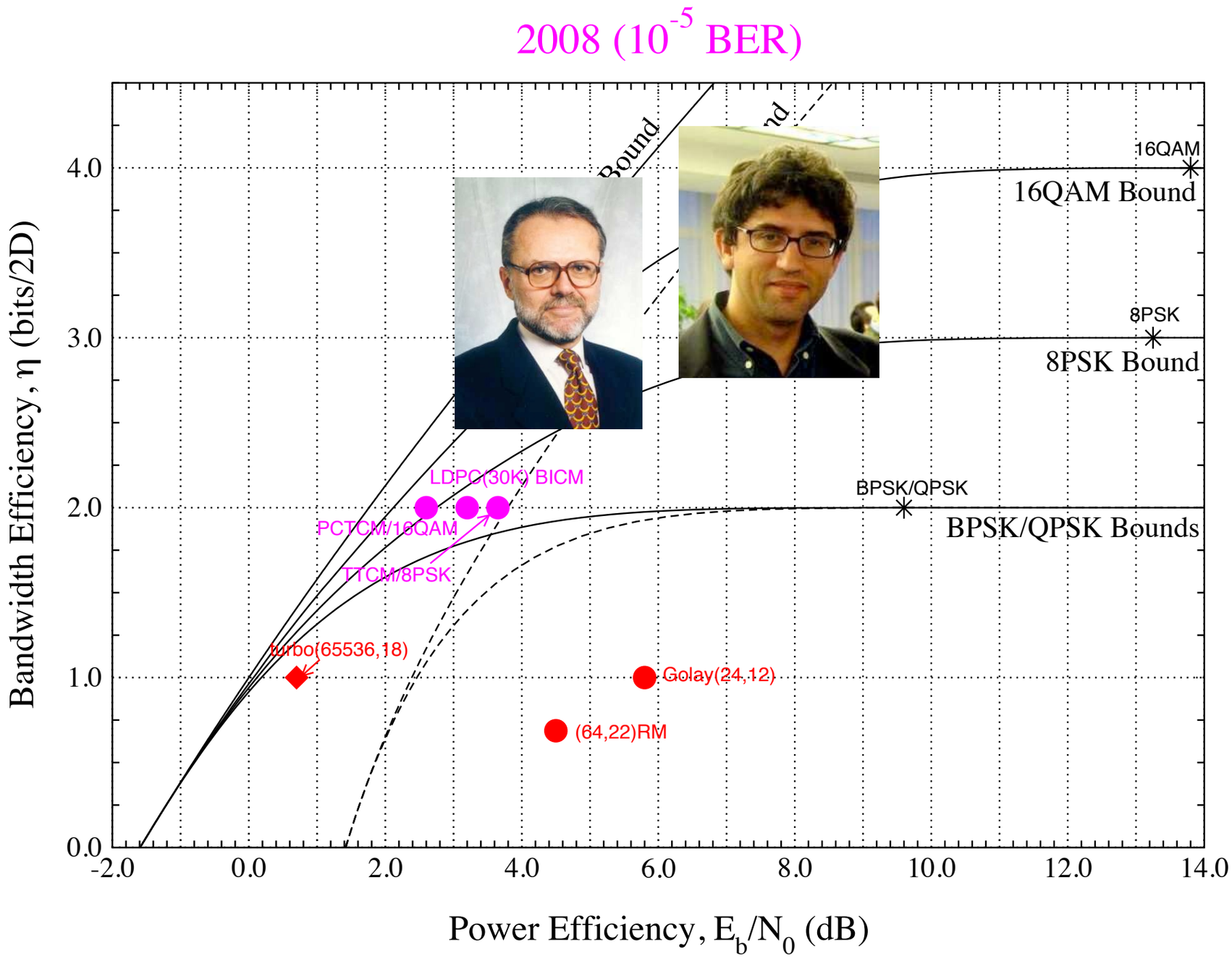


Parallel concatenated TCM is a turbo coding system with trellis coded modulation component codes.

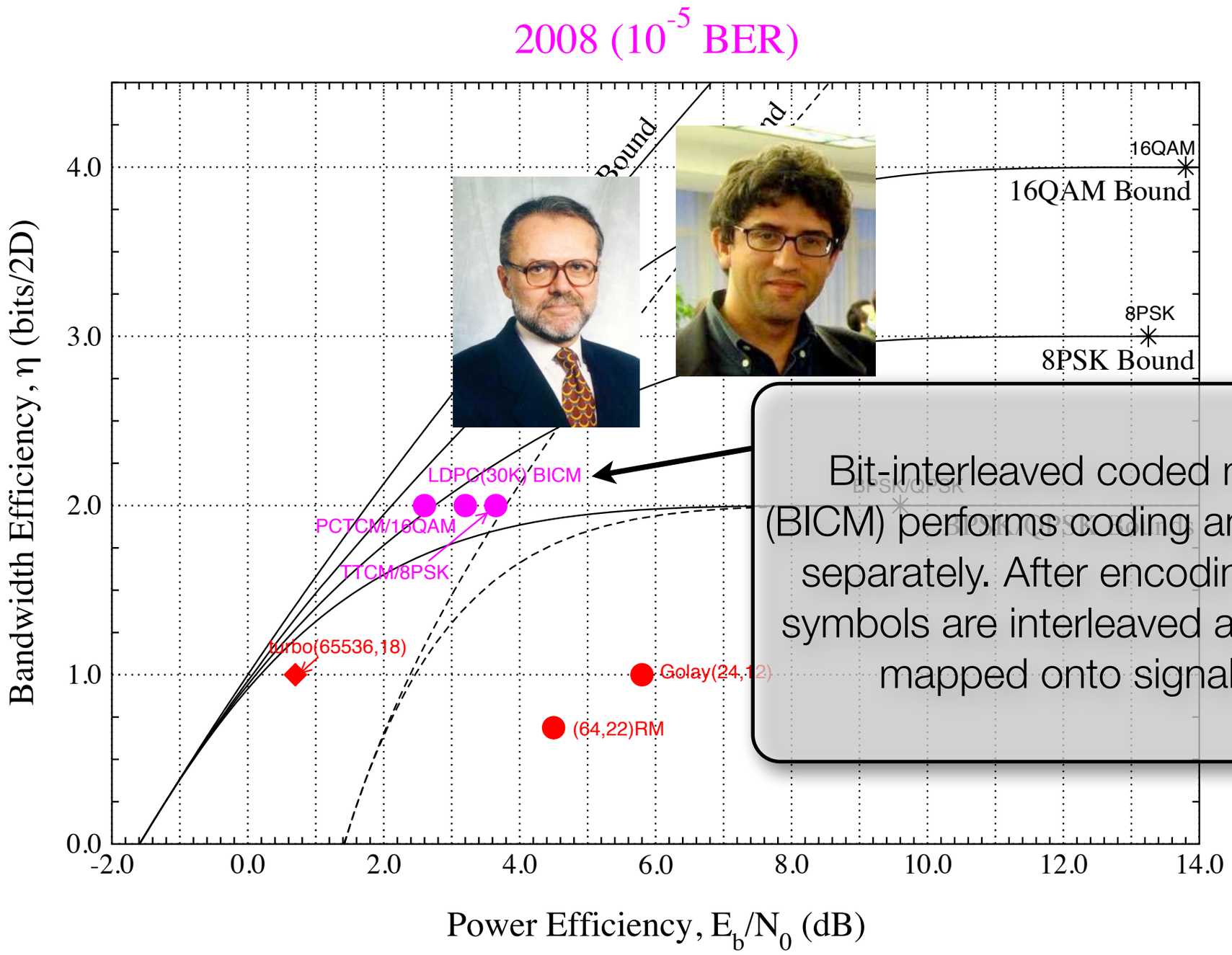
The Sixth Day



The Sixth Day

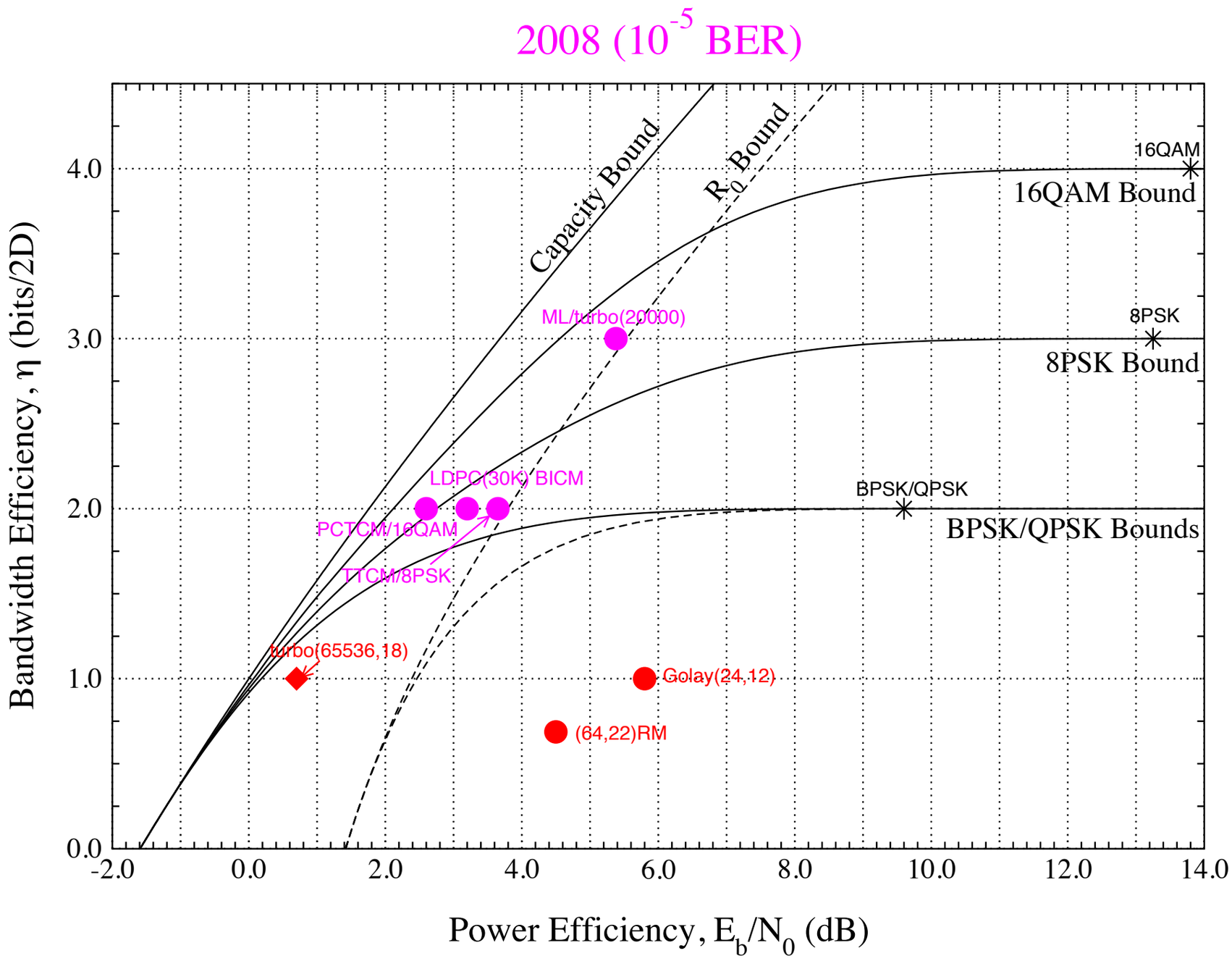


The Sixth Day

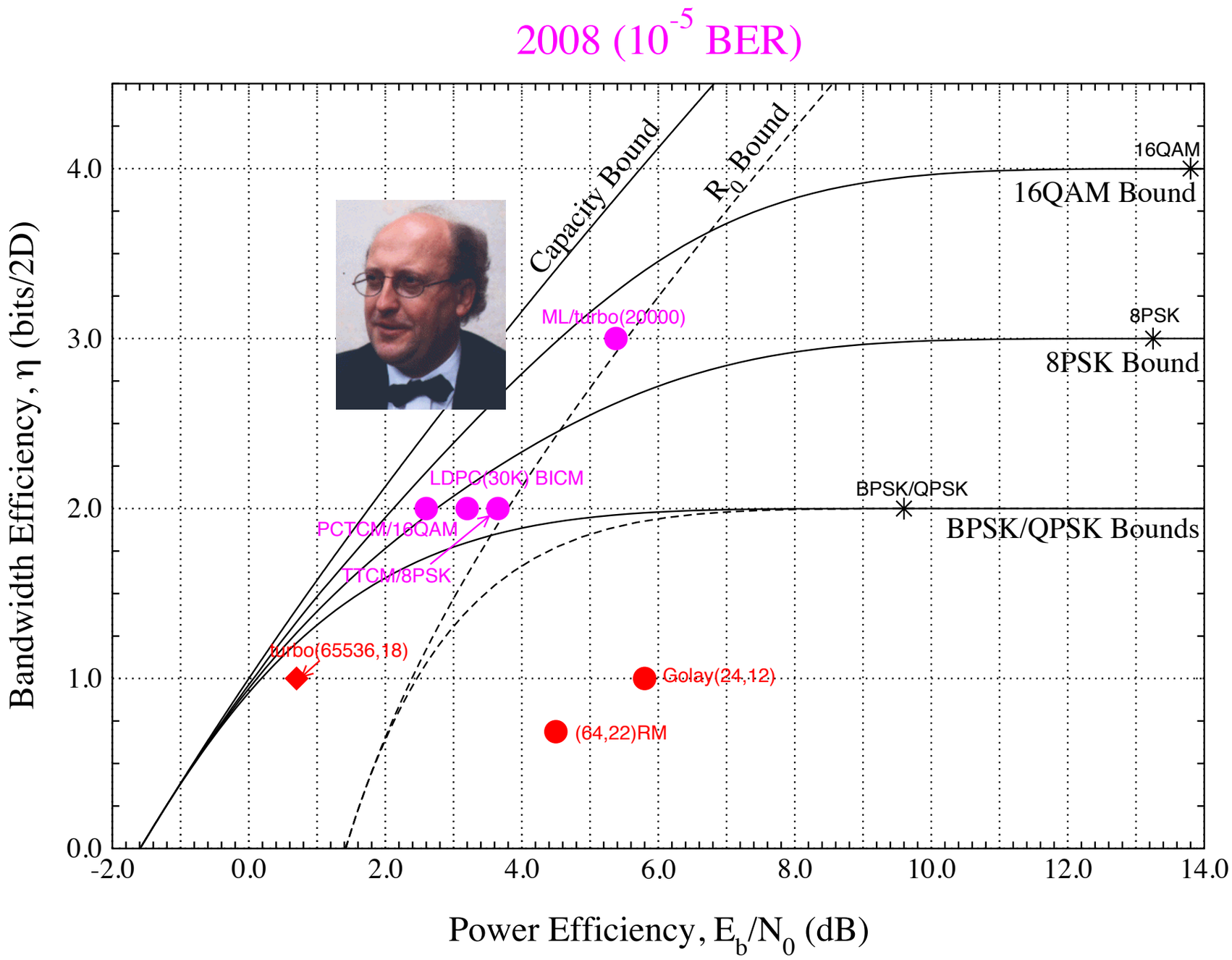


Bit-interleaved coded modulation (BICM) performs coding and modulation separately. After encoding, the code symbols are interleaved and then Gray mapped onto signal points.

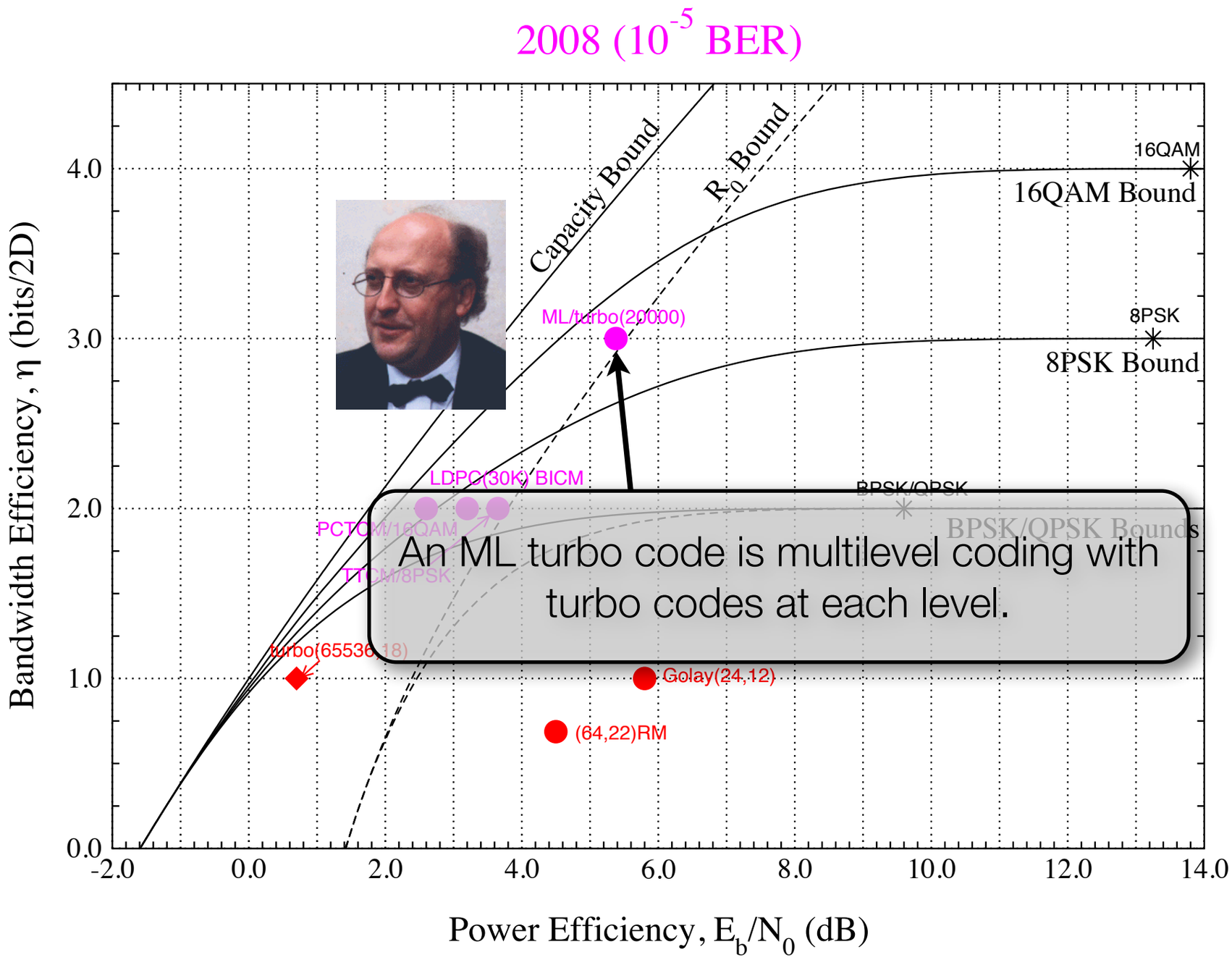
The Sixth Day



The Sixth Day

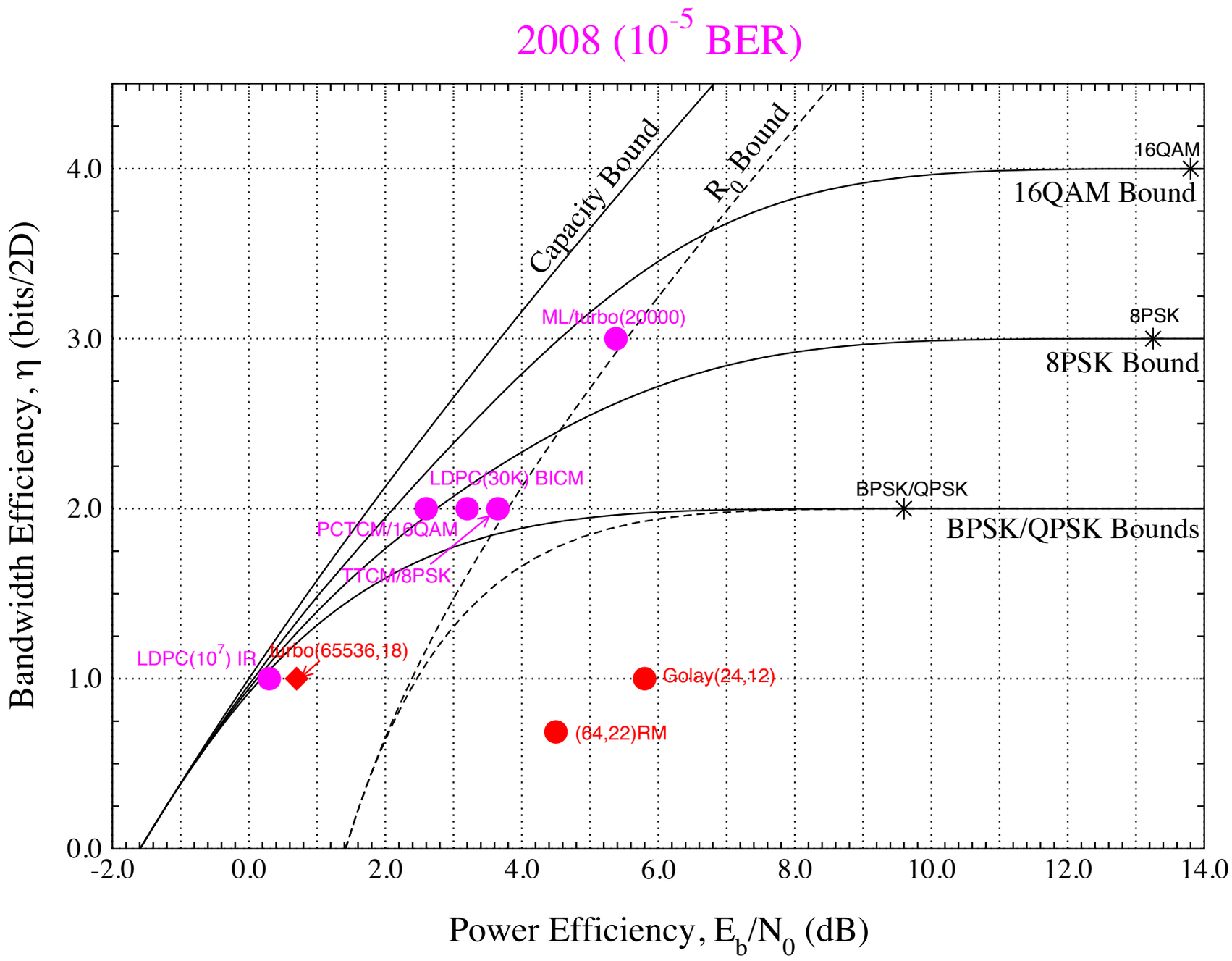


The Sixth Day

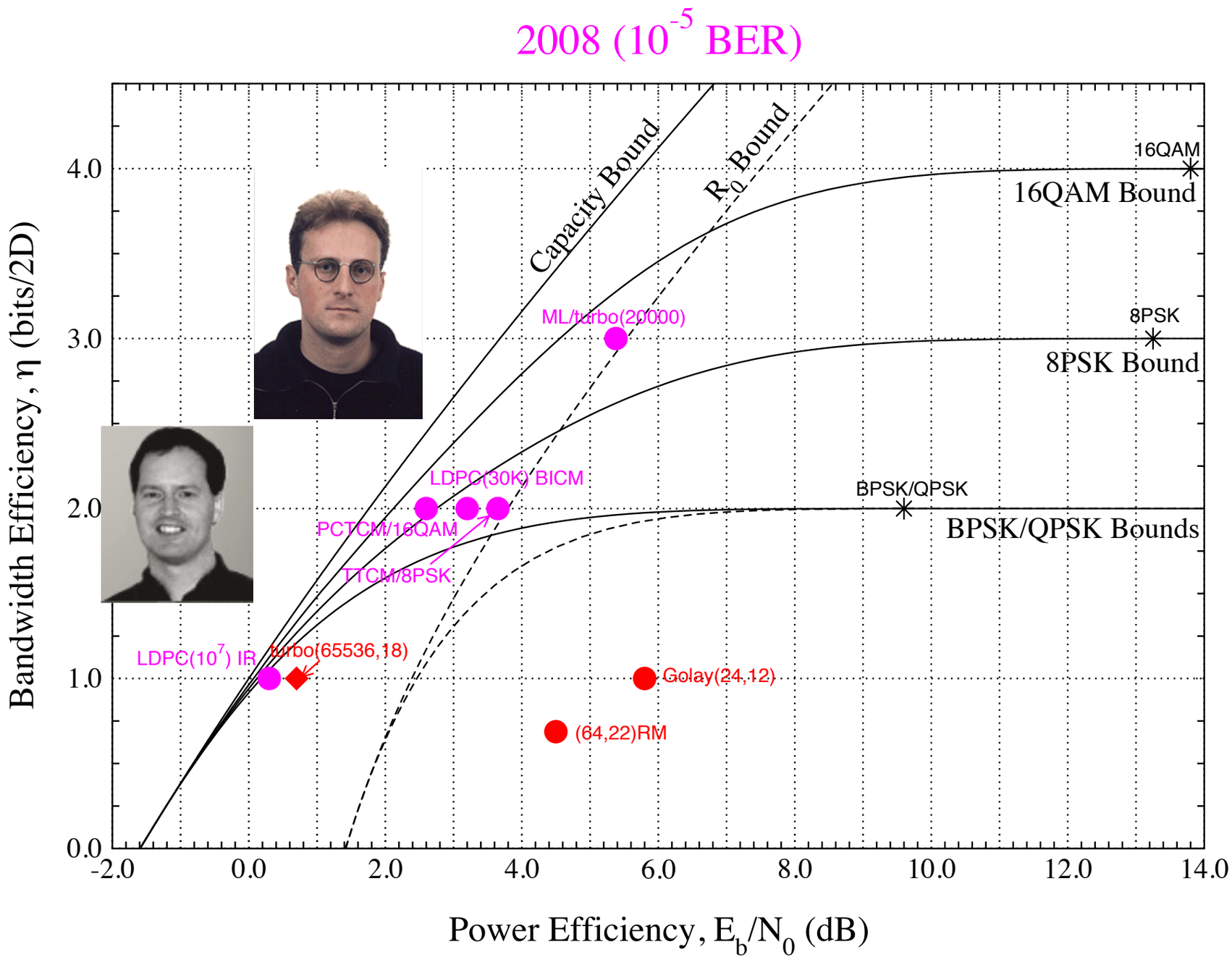


An ML turbo code is multilevel coding with turbo codes at each level.

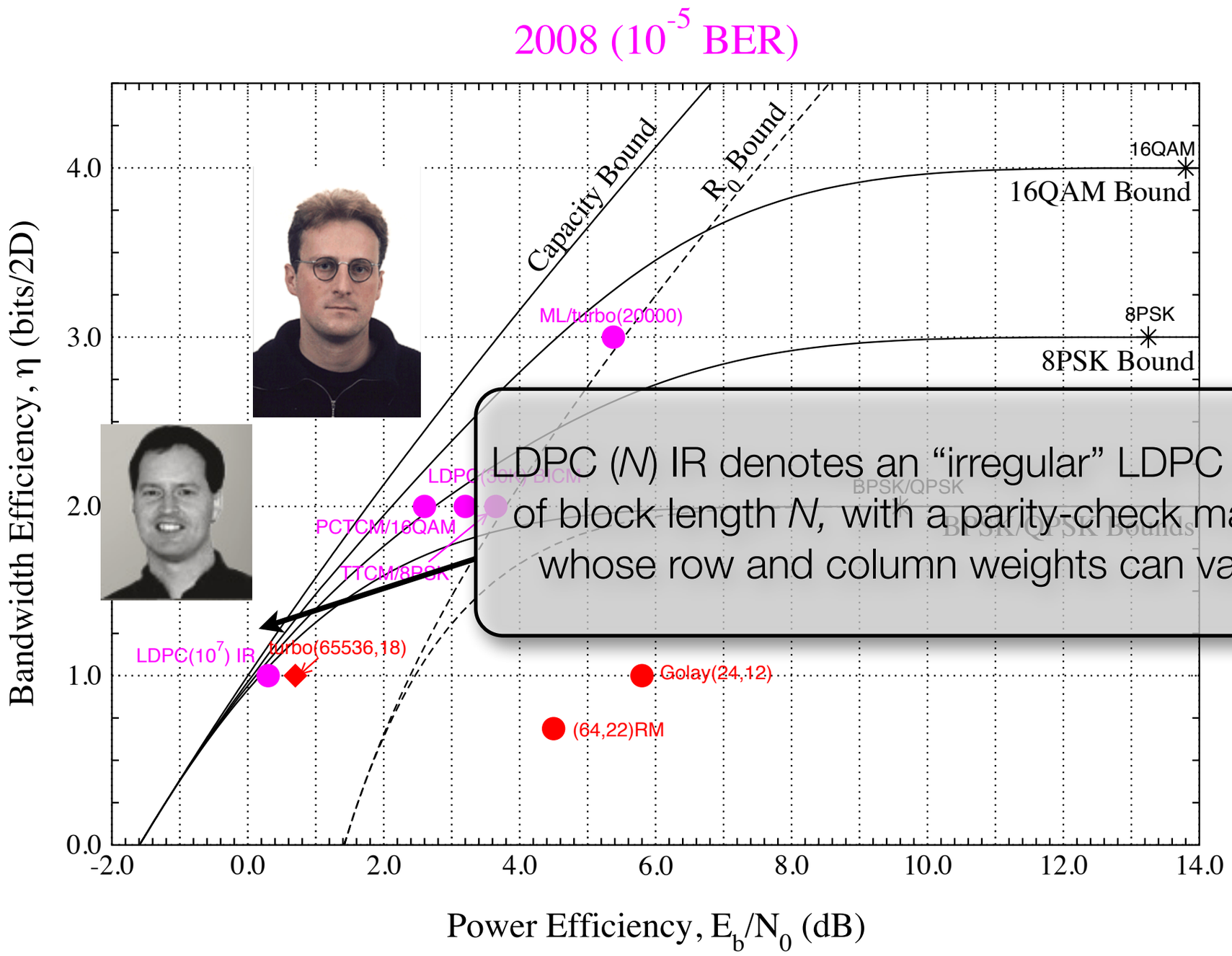
The Sixth Day



The Sixth Day

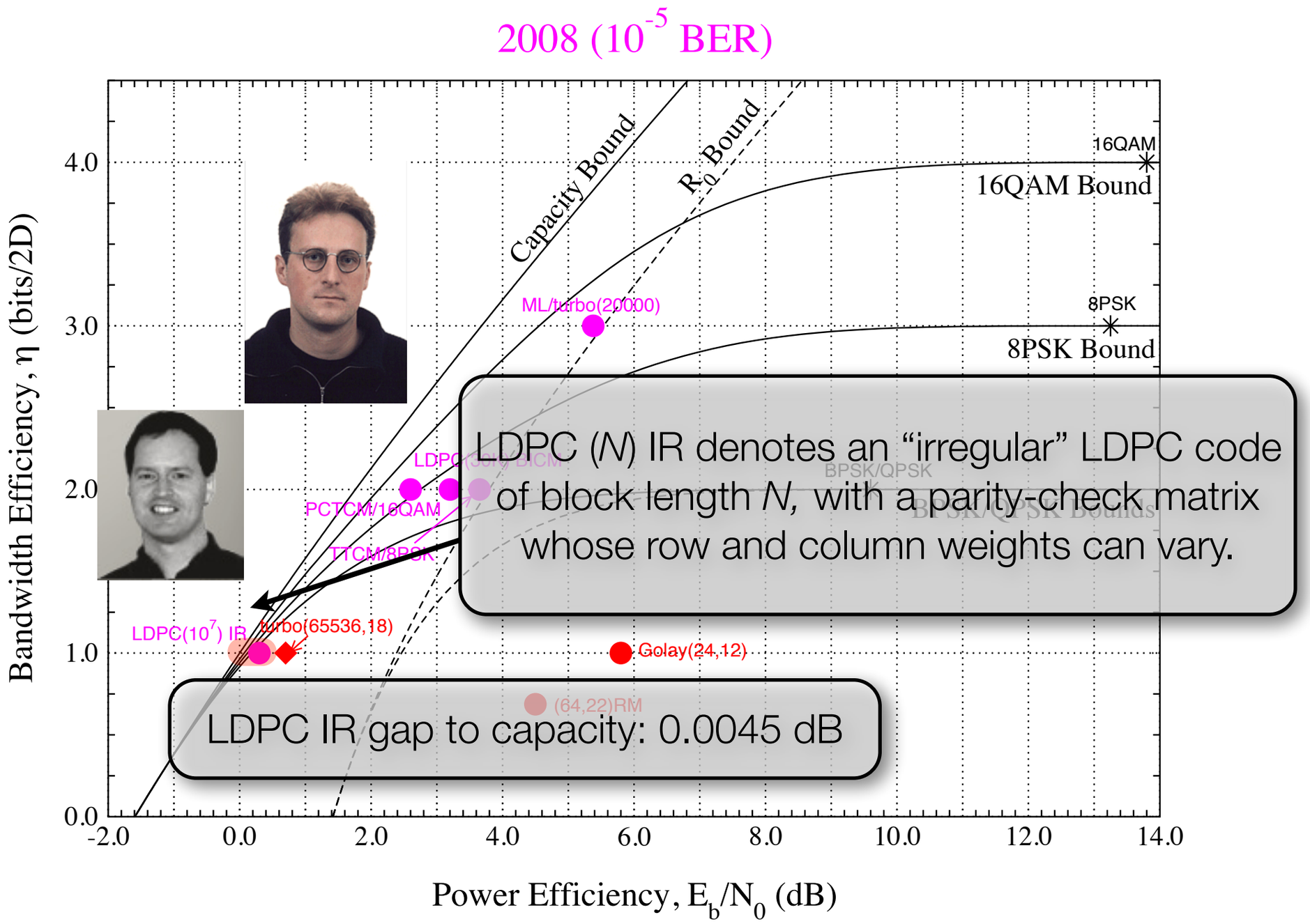


The Sixth Day



LDPC (*N*) IR denotes an "irregular" LDPC code of block length *N*, with a parity-check matrix whose row and column weights can vary.

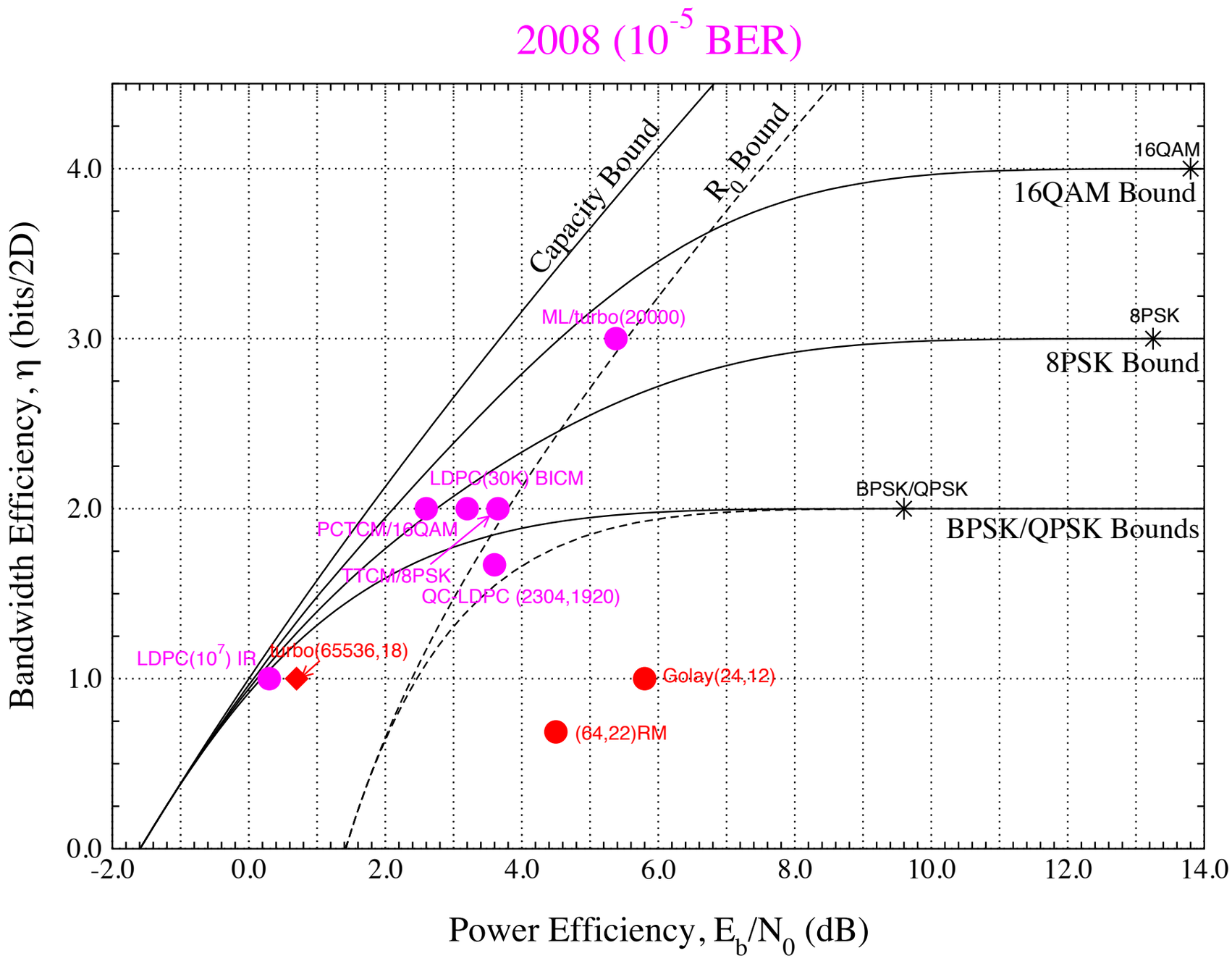
The Sixth Day



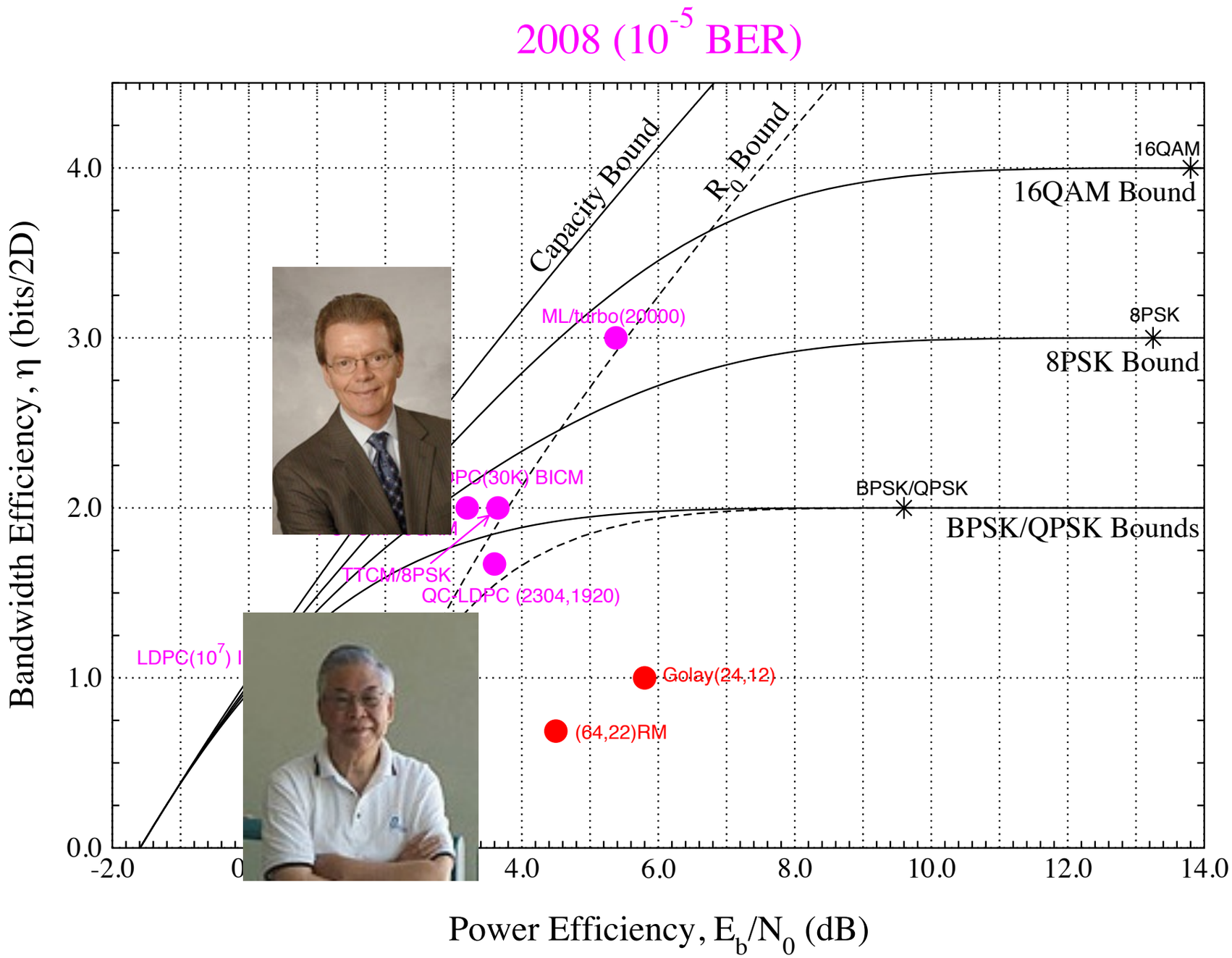
LDPC (*N*) IR denotes an "irregular" LDPC code of block length *N*, with a parity-check matrix whose row and column weights can vary.

LDPC IR gap to capacity: 0.0045 dB

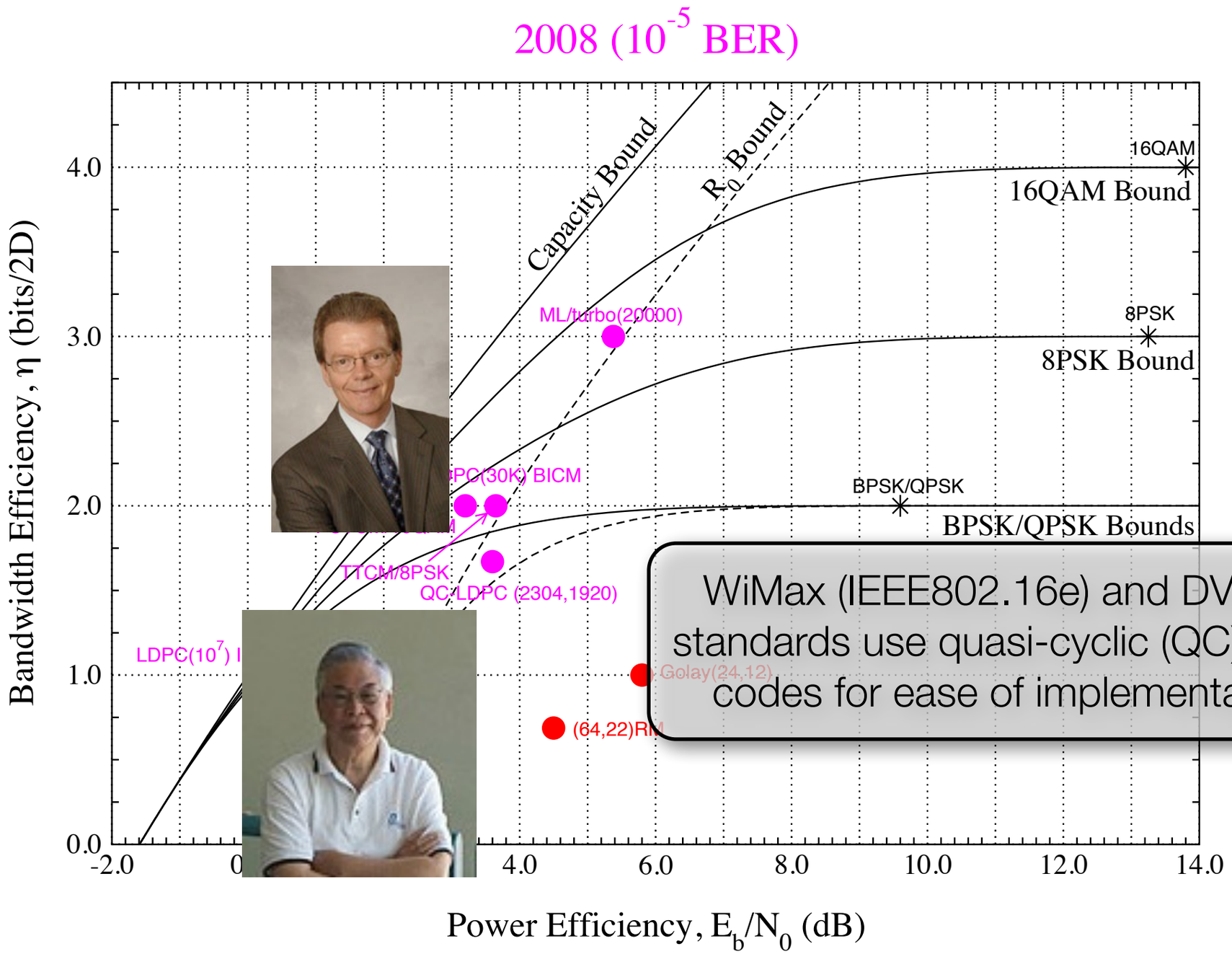
The Sixth Day



The Sixth Day

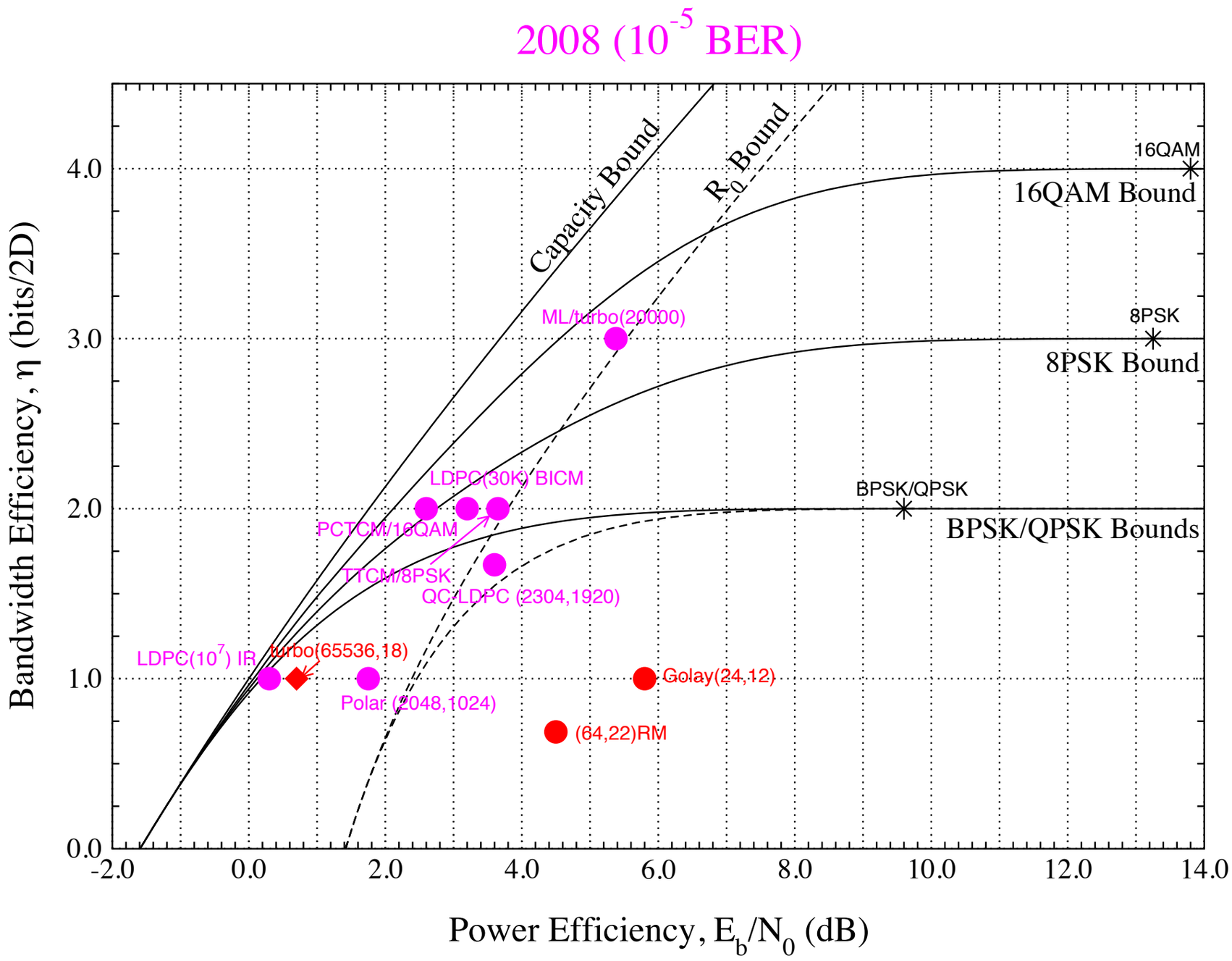


The Sixth Day

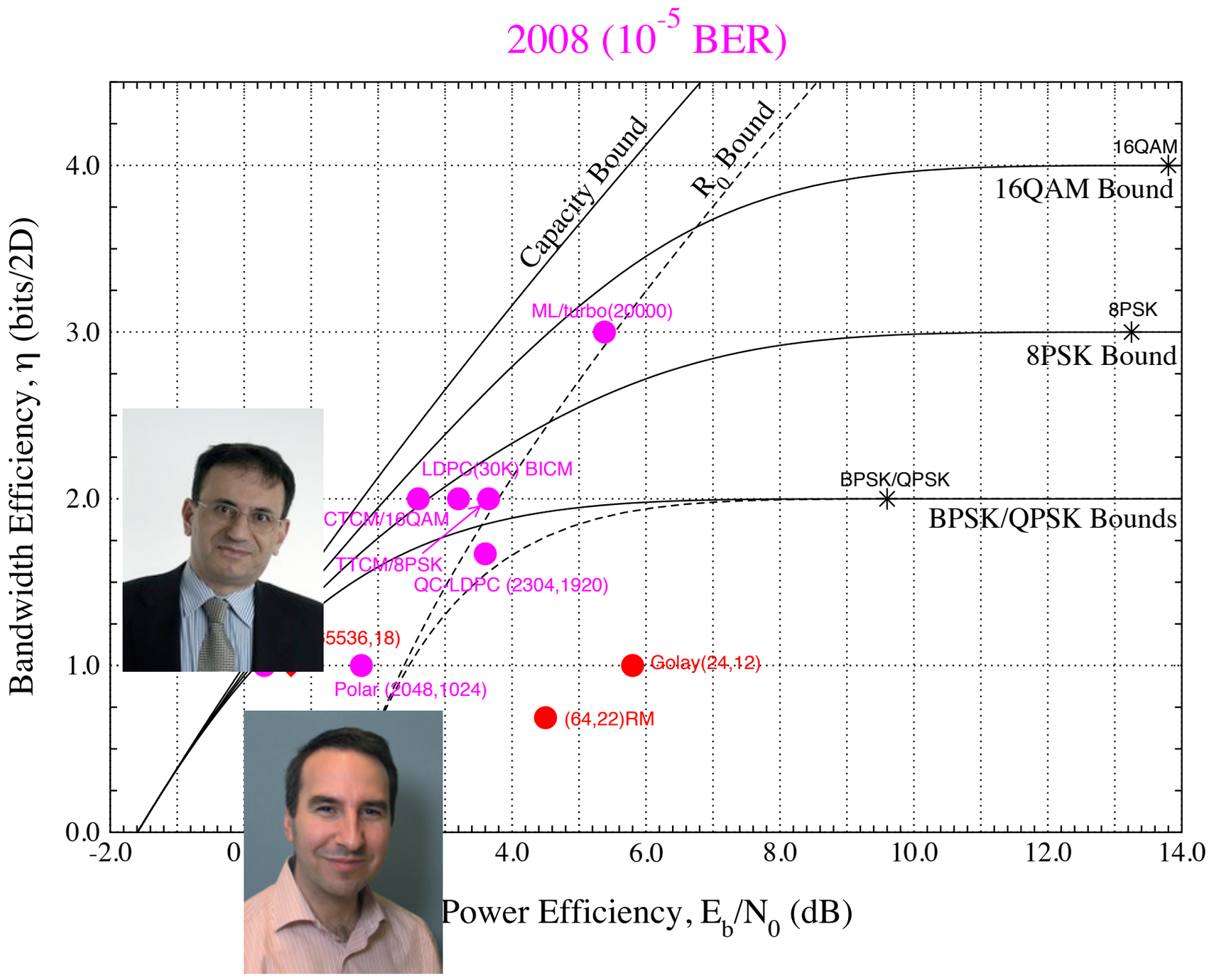


WiMax (IEEE802.16e) and DVB-S2 standards use quasi-cyclic (QC) LDPC codes for ease of implementation.

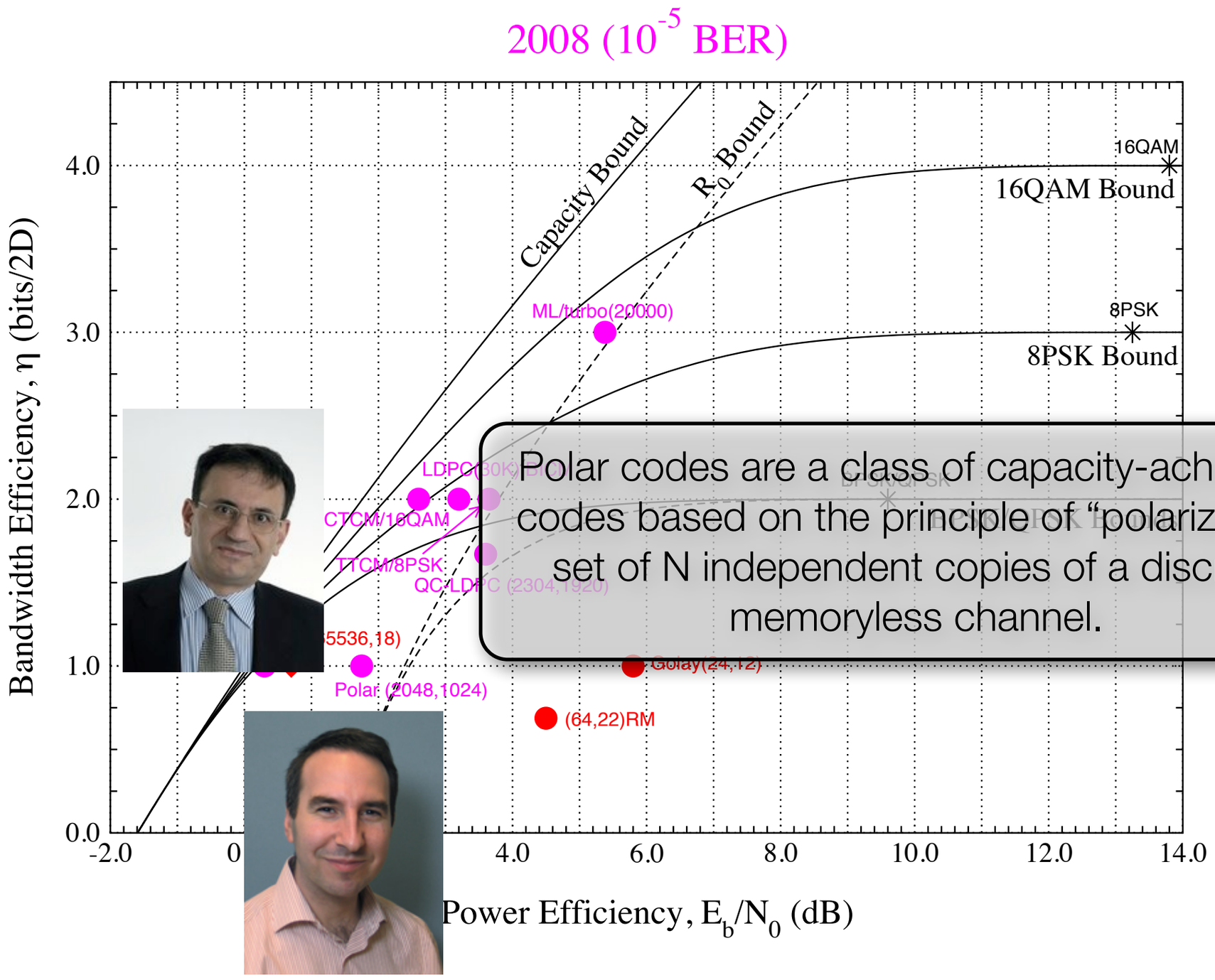
The Sixth Day



The Sixth Day

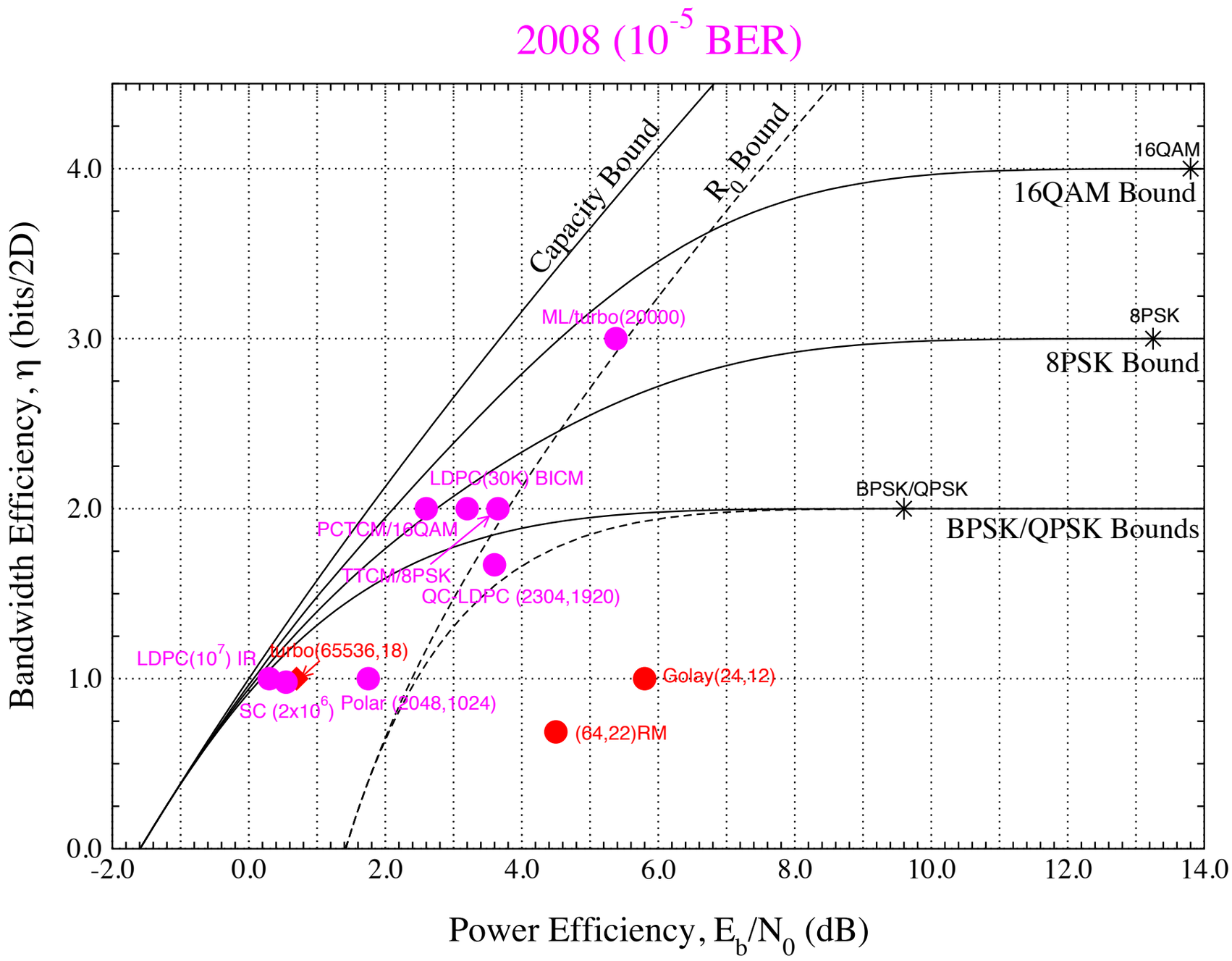


The Sixth Day

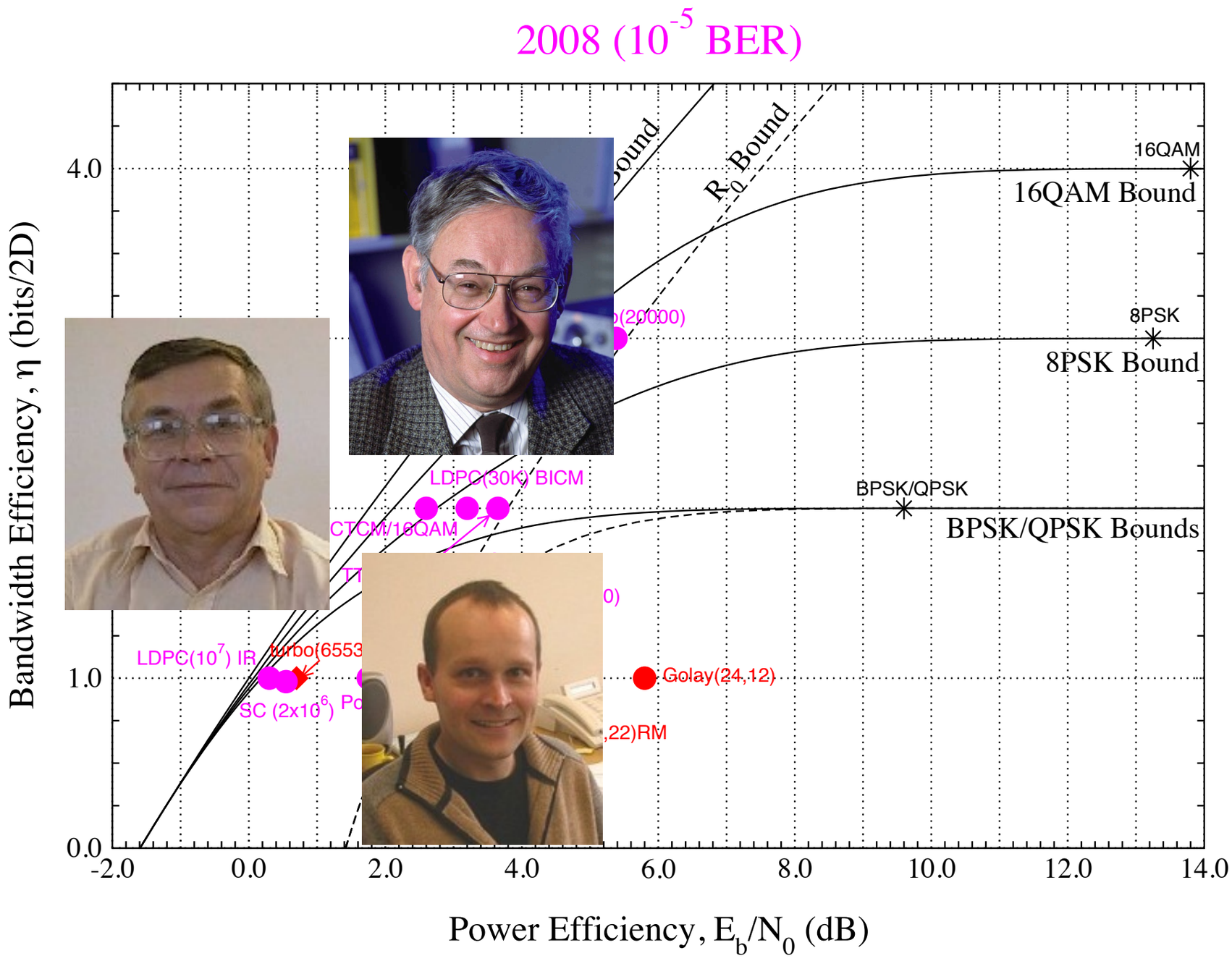


Polar codes are a class of capacity-achieving codes based on the principle of "polarizing" a set of N independent copies of a discrete memoryless channel.

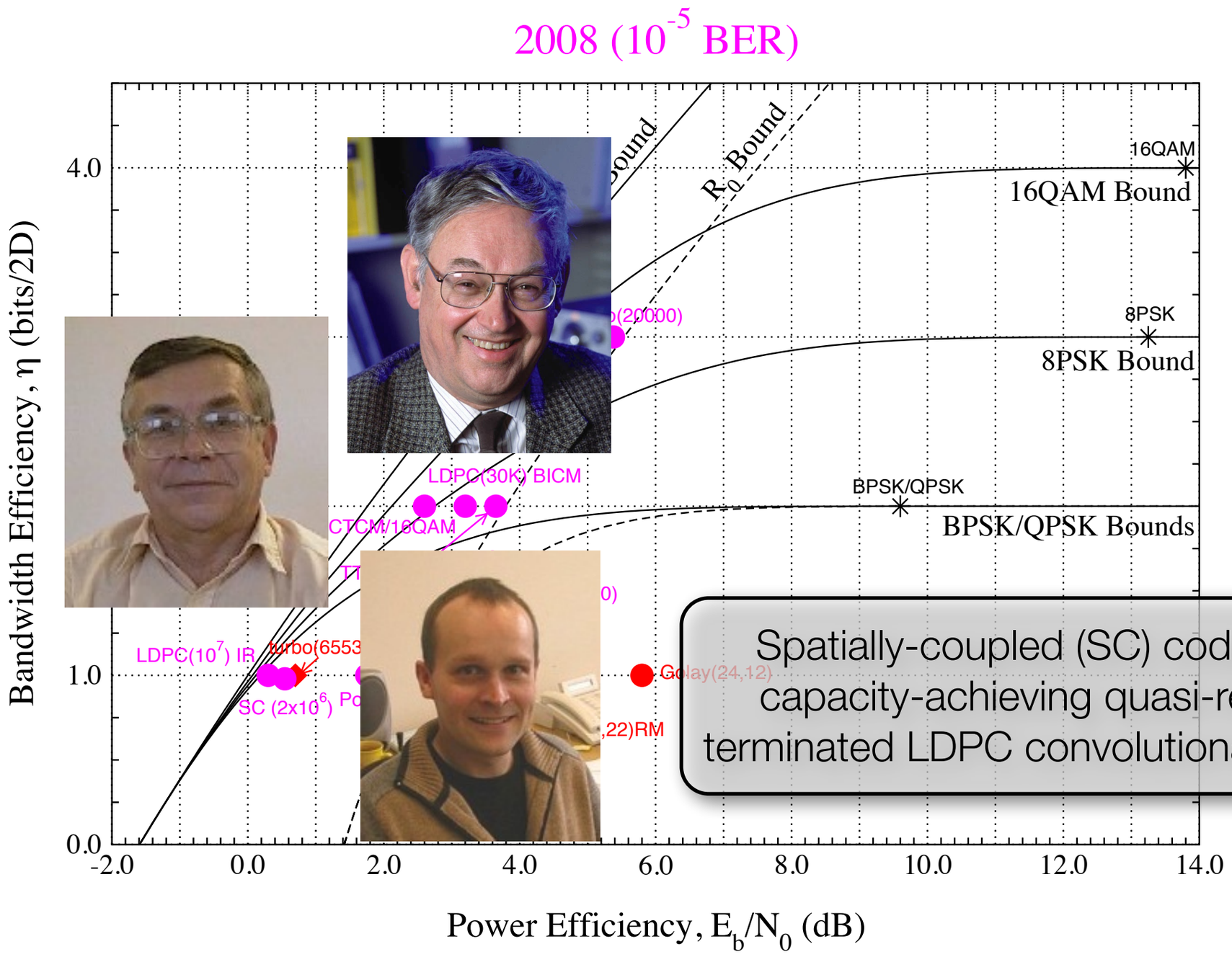
The Sixth Day



The Sixth Day

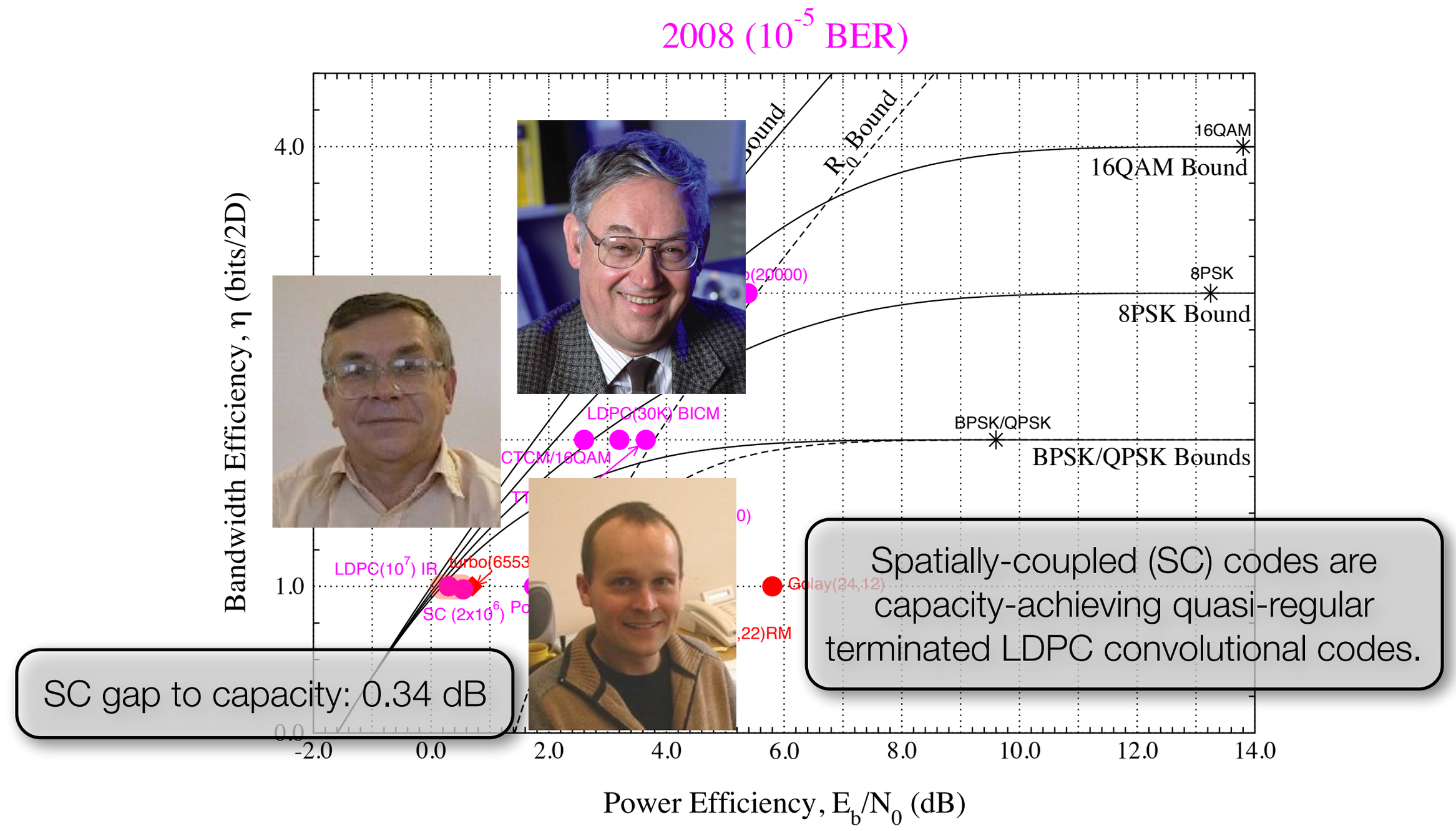


The Sixth Day

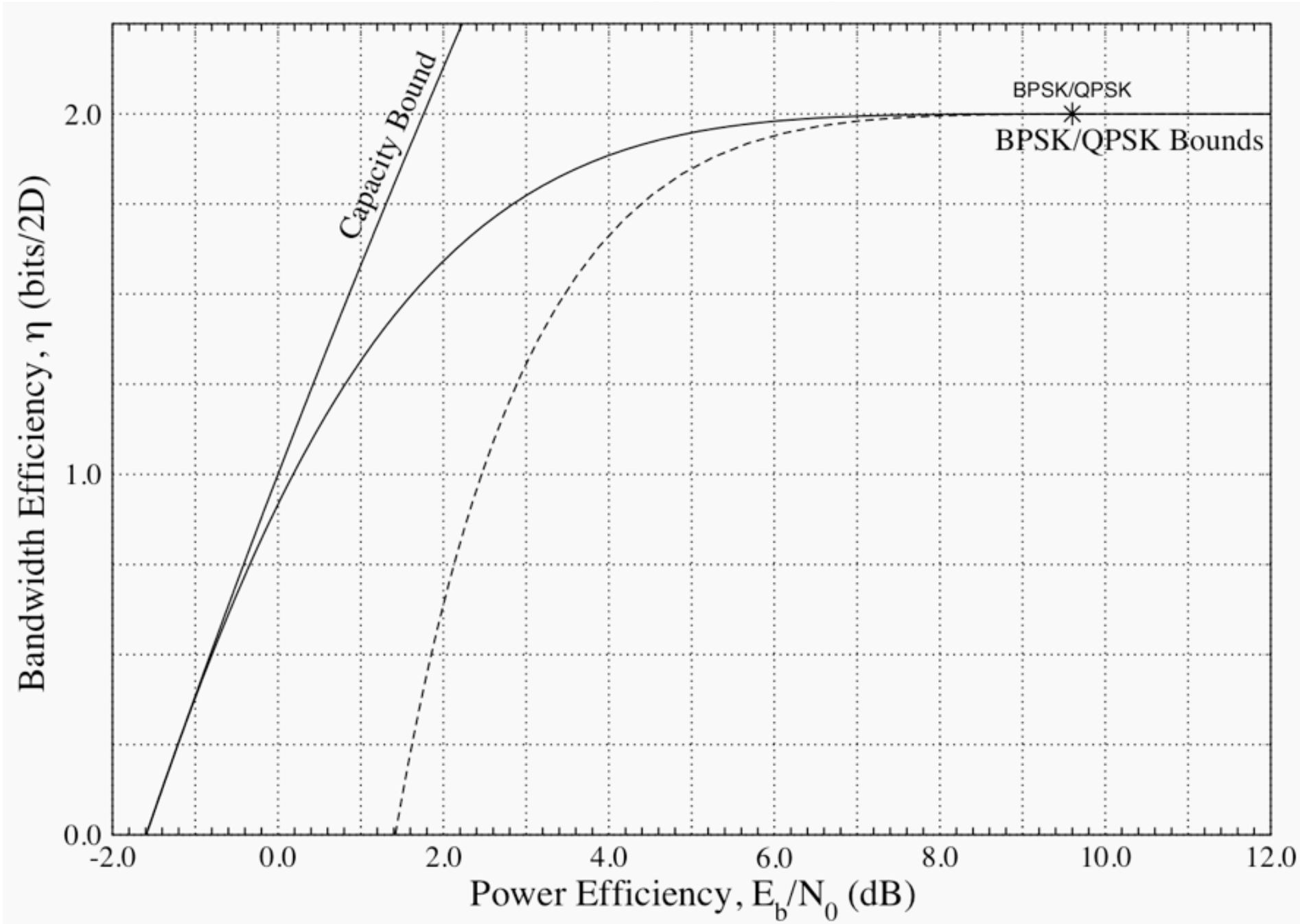


Spatially-coupled (SC) codes are capacity-achieving quasi-regular terminated LDPC convolutional codes.

The Sixth Day

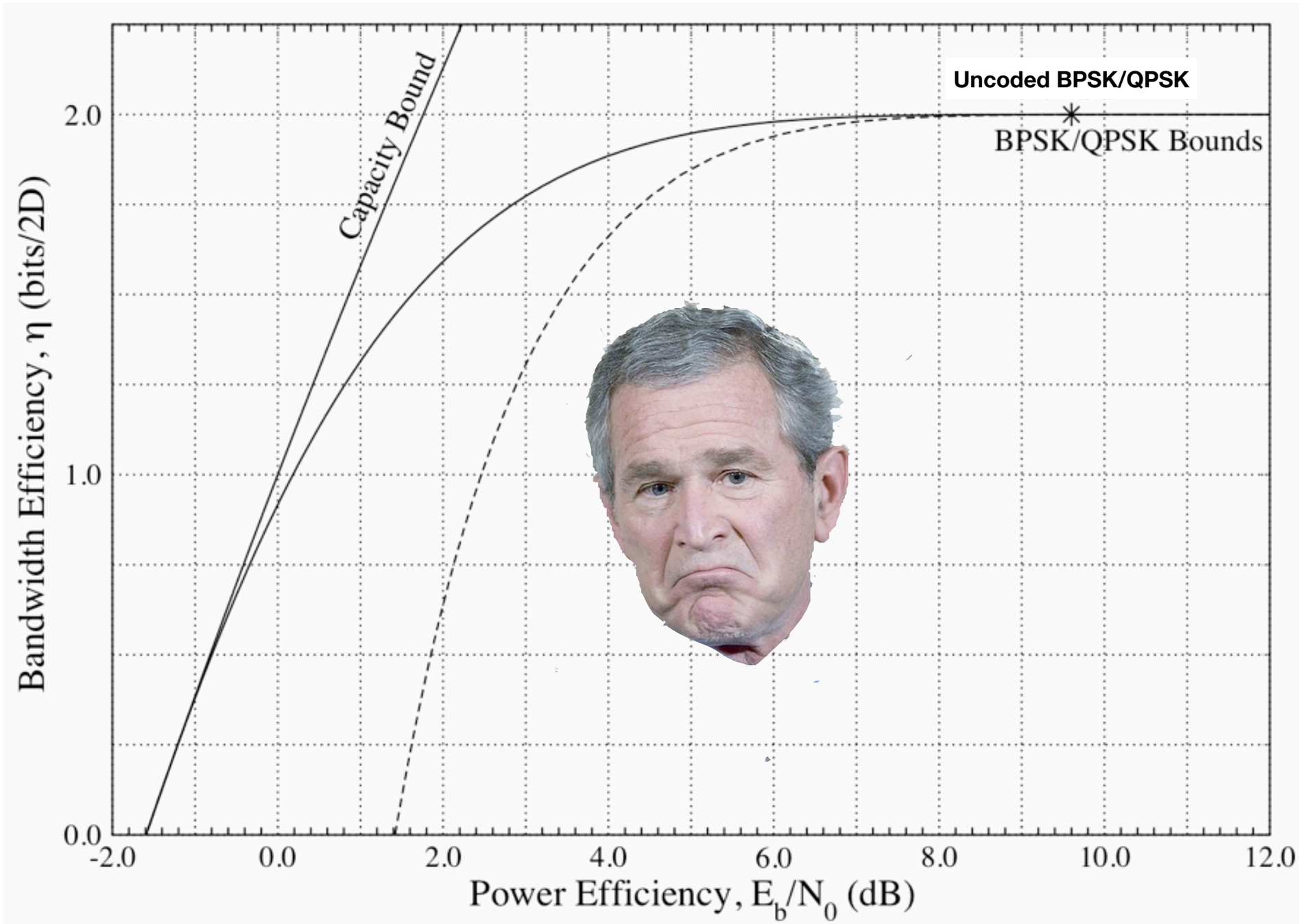


Political Views on Coding Theory



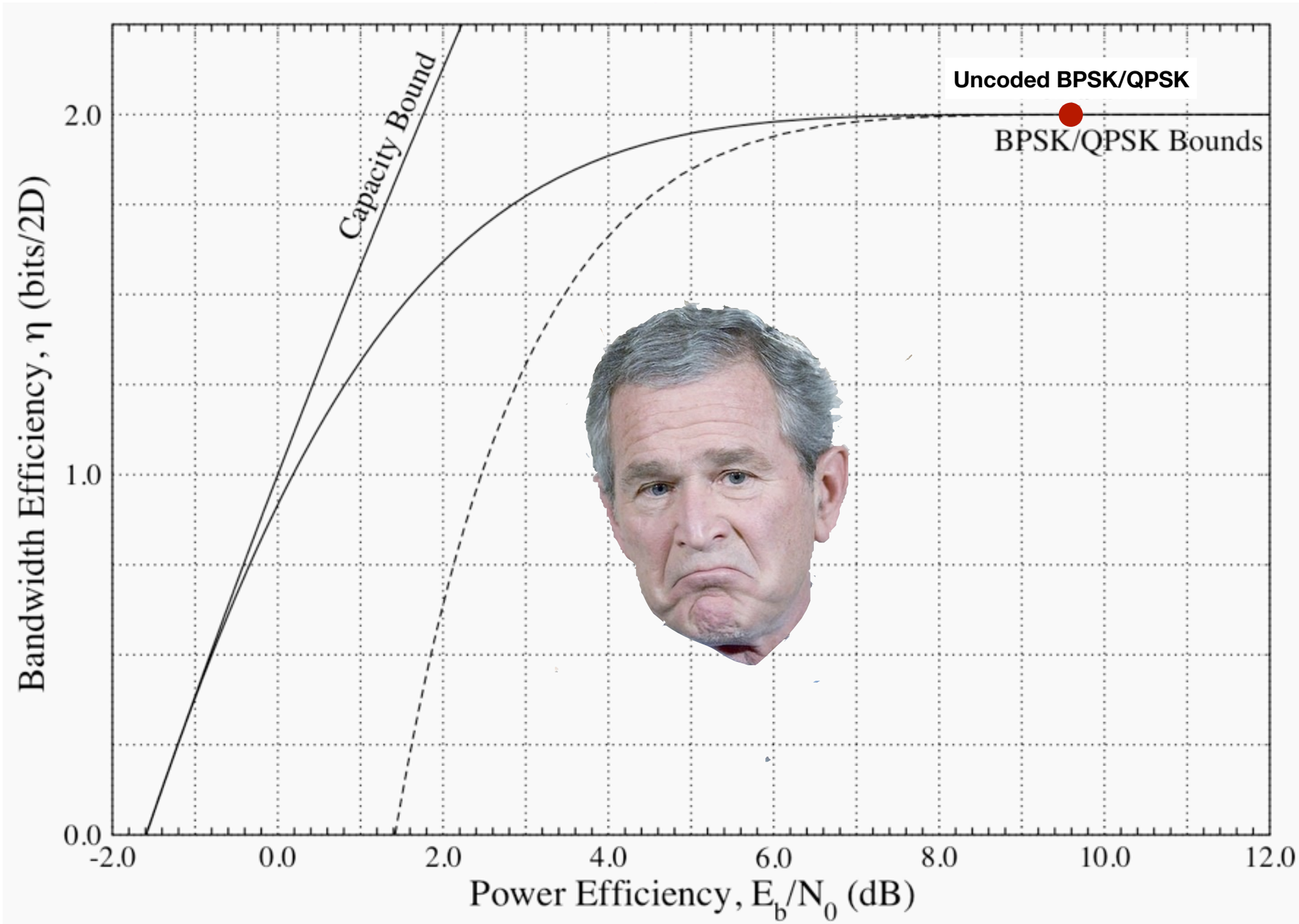
Political Views on Coding Theory

George W. Bush - *US President (2000-2008)*



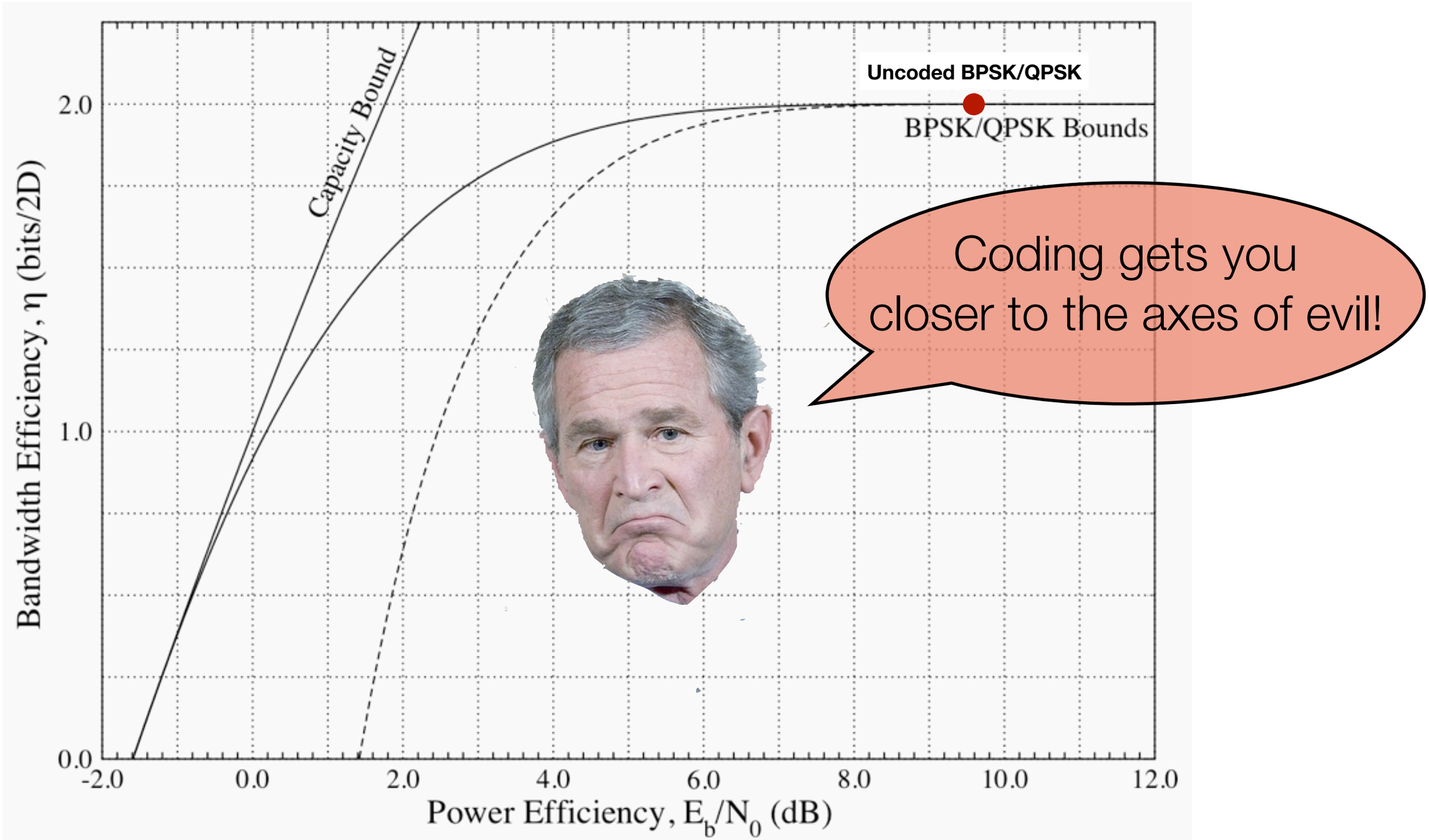
Political Views on Coding Theory

George W. Bush - *US President (2000-2008)*



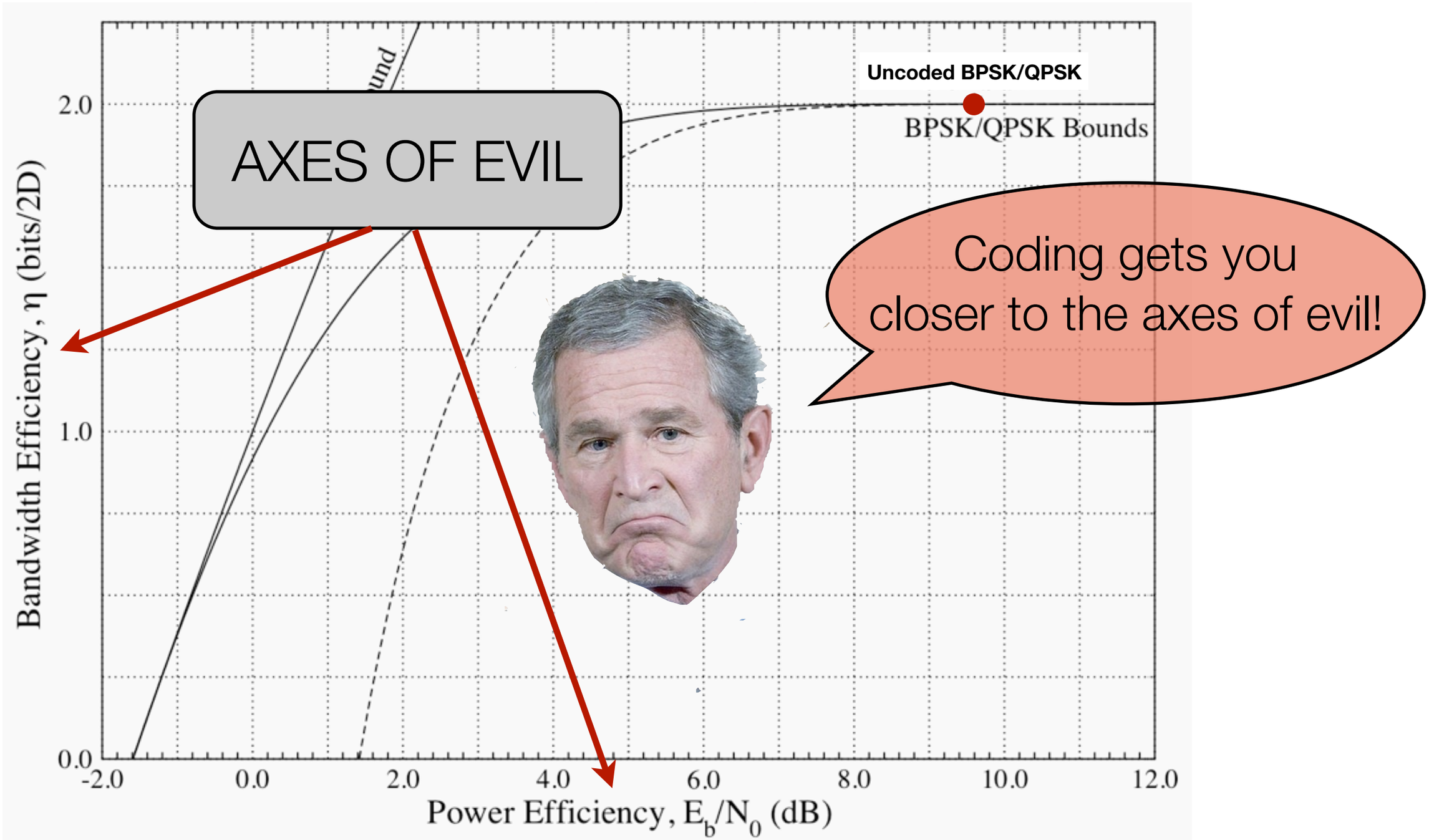
Political Views on Coding Theory

George W. Bush - *US President (2000-2008)*



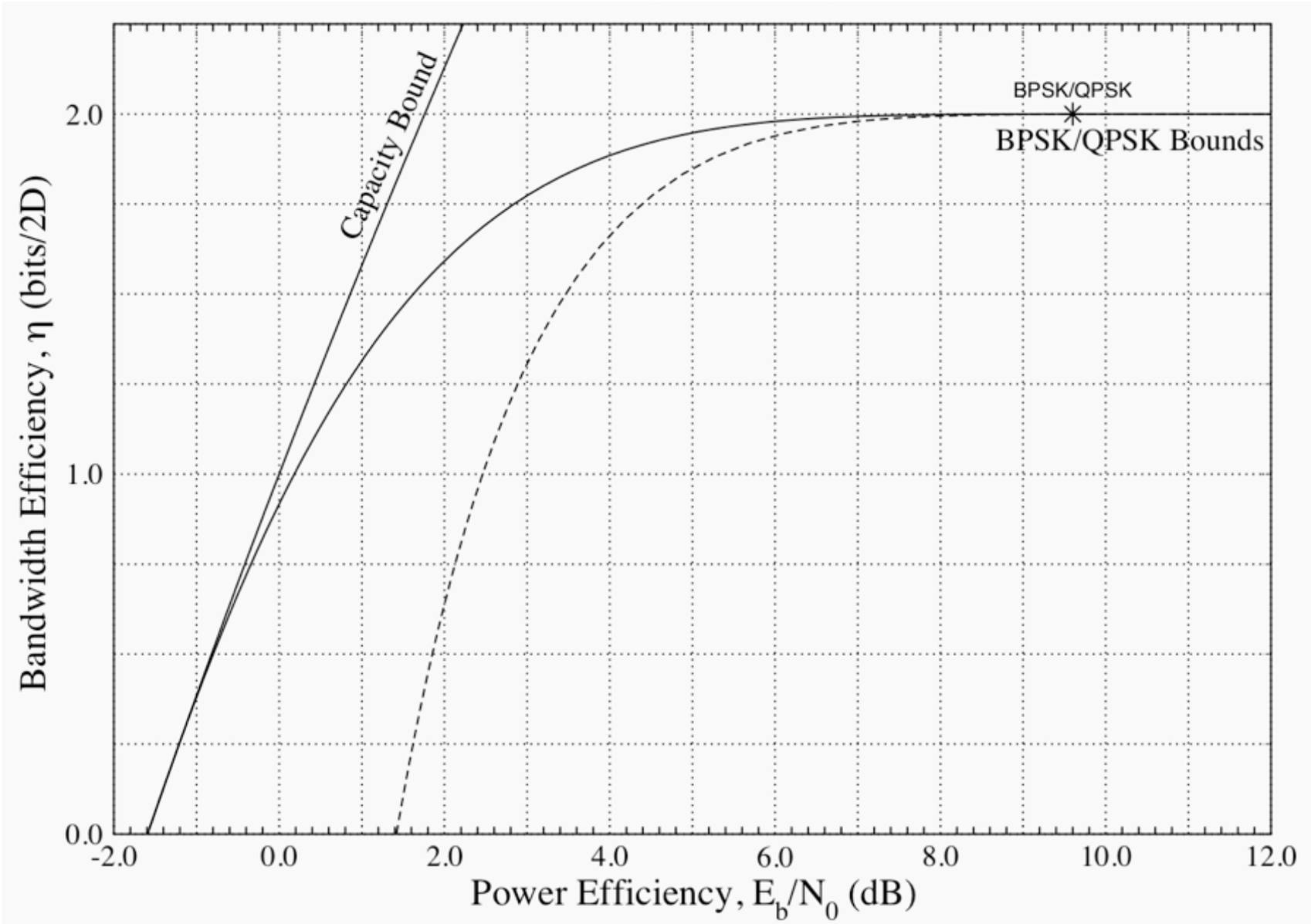
Political Views on Coding Theory

George W. Bush - *US President (2000-2008)*



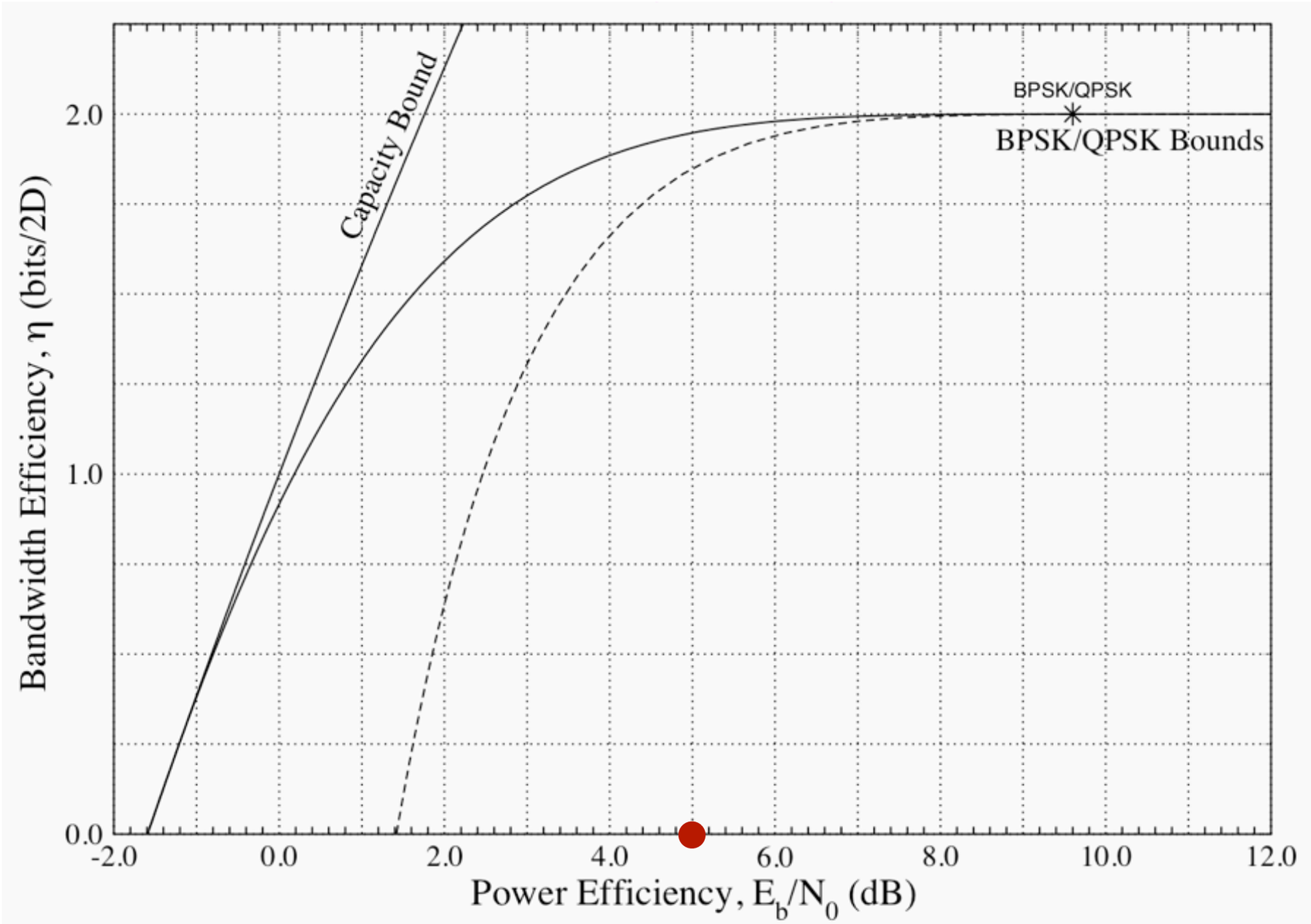
Political Views on Coding Theory

Joe Biden - *US Vice-President (2008-2016)*



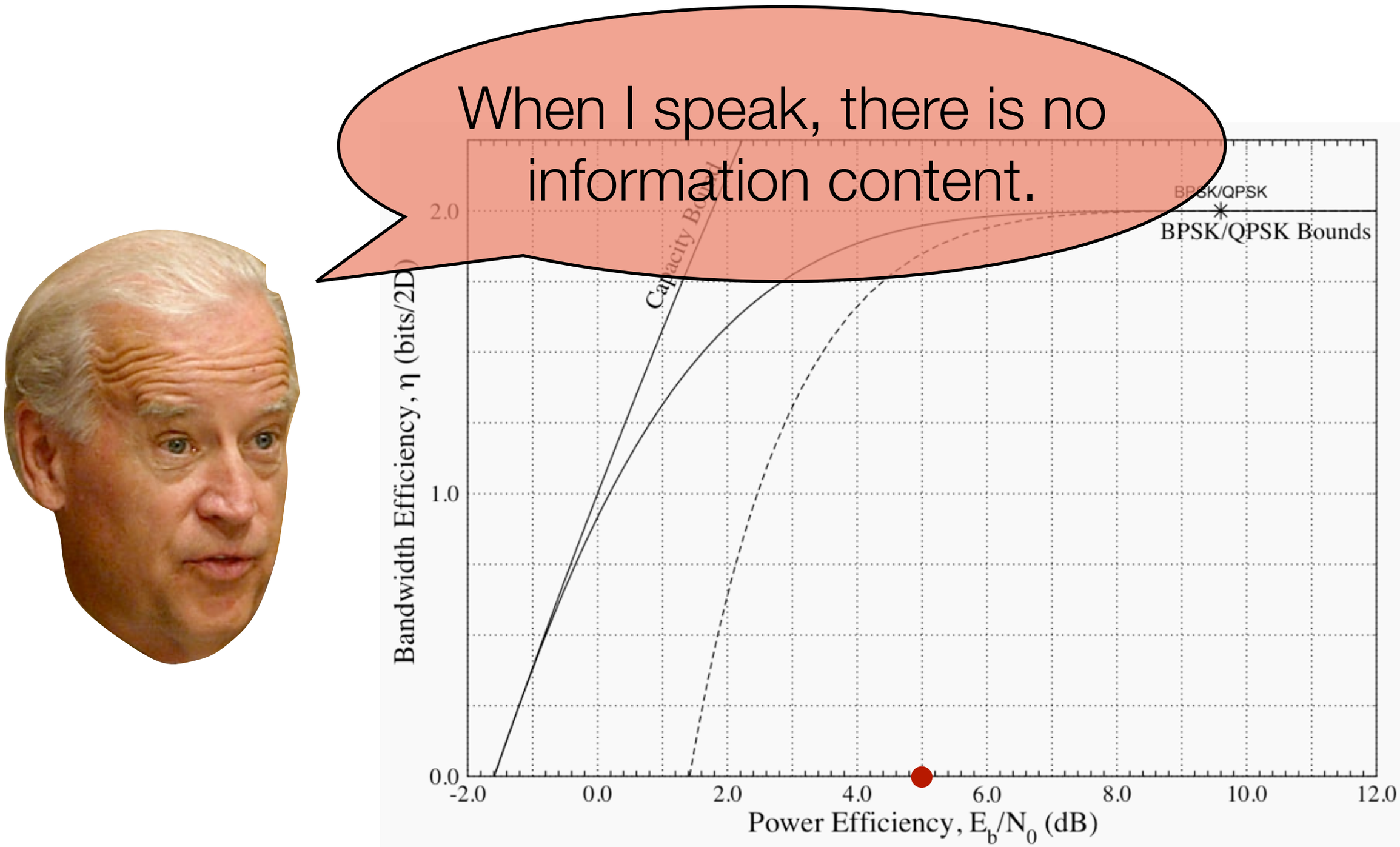
Political Views on Coding Theory

Joe Biden - *US Vice-President (2008-2016)*



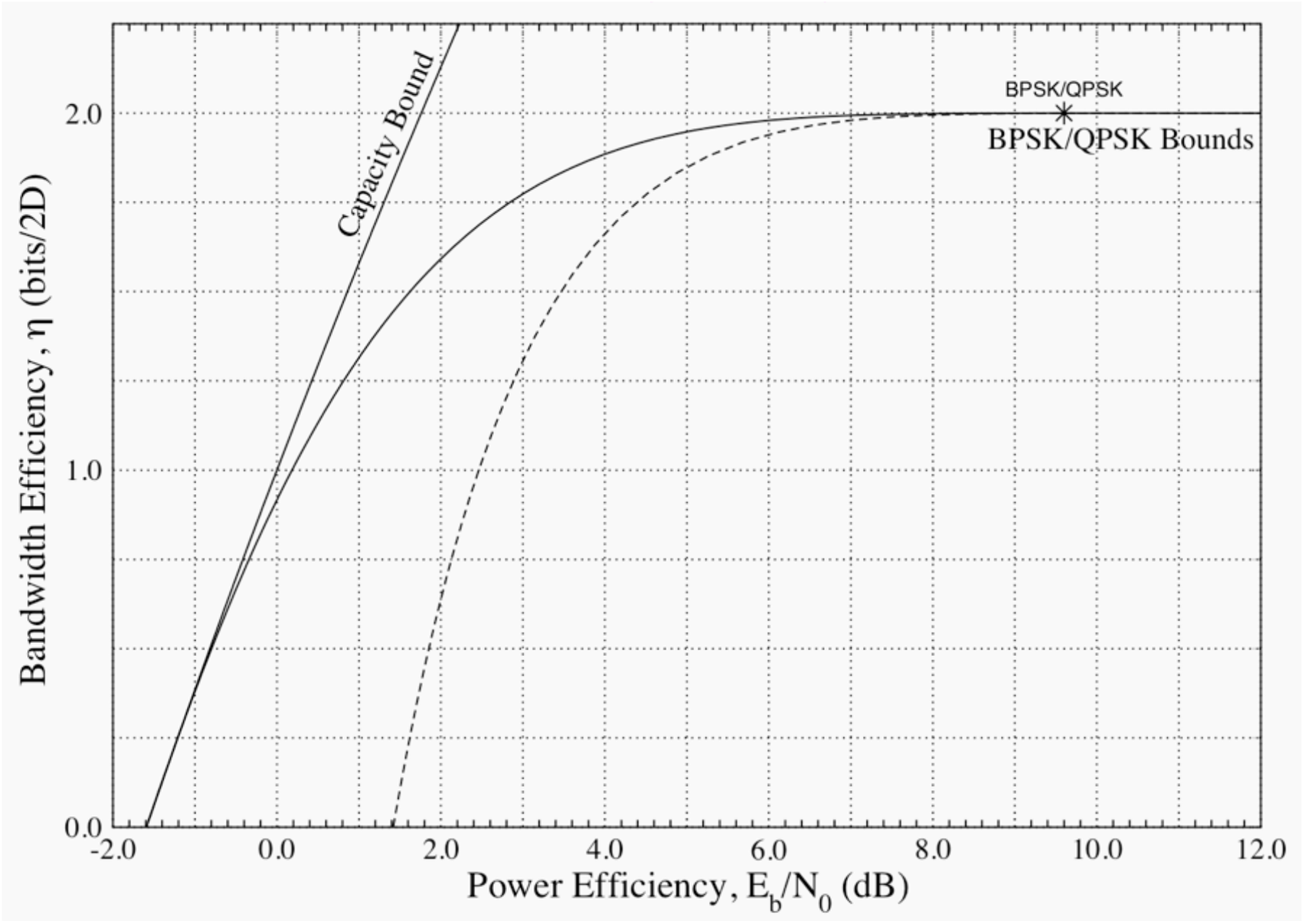
Political Views on Coding Theory

Joe Biden - *US Vice-President (2008-2016)*



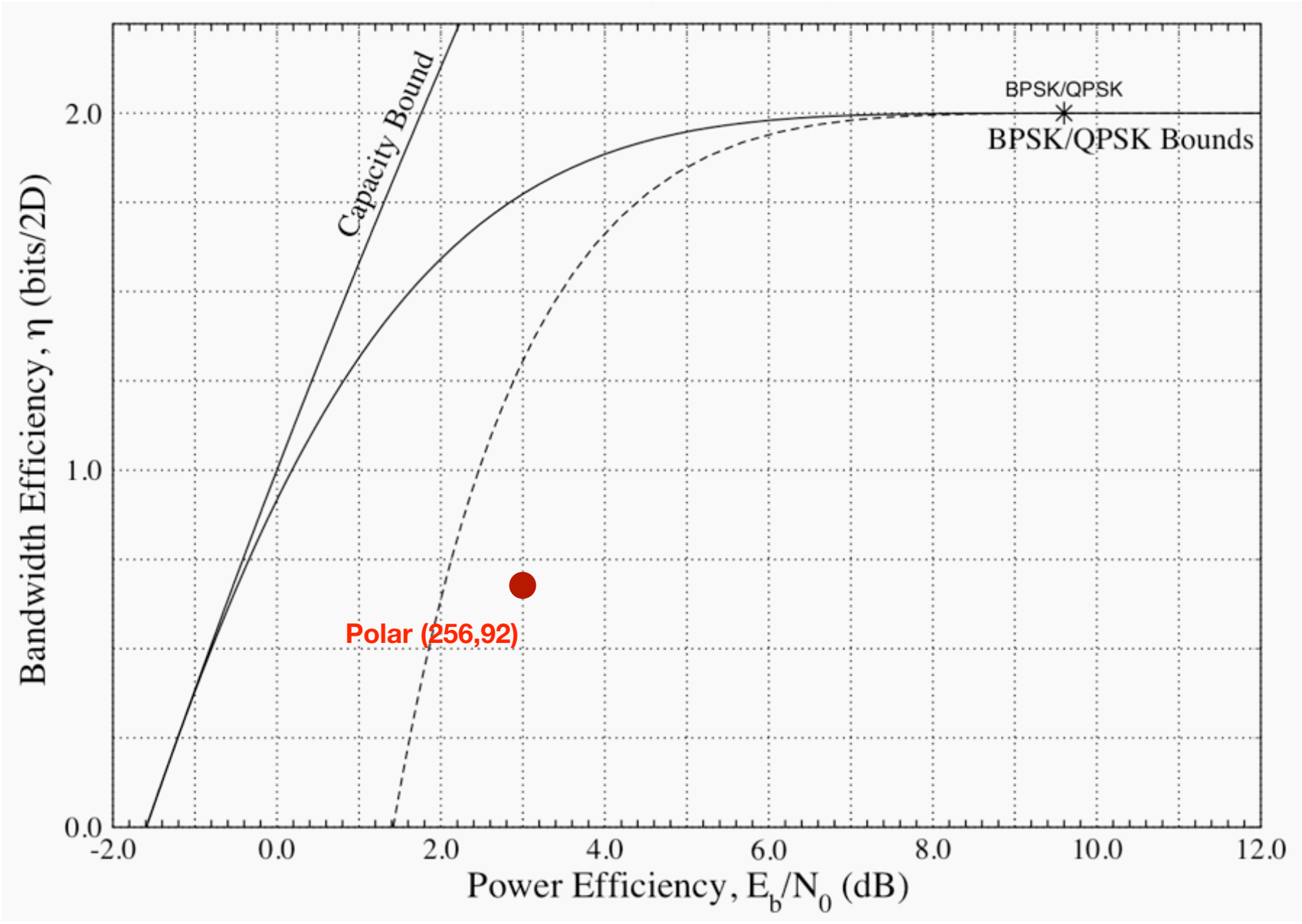
Political Views on Coding Theory

Sarah Palin - *US Vice-Presidential Candidate (2008)*



Political Views on Coding Theory

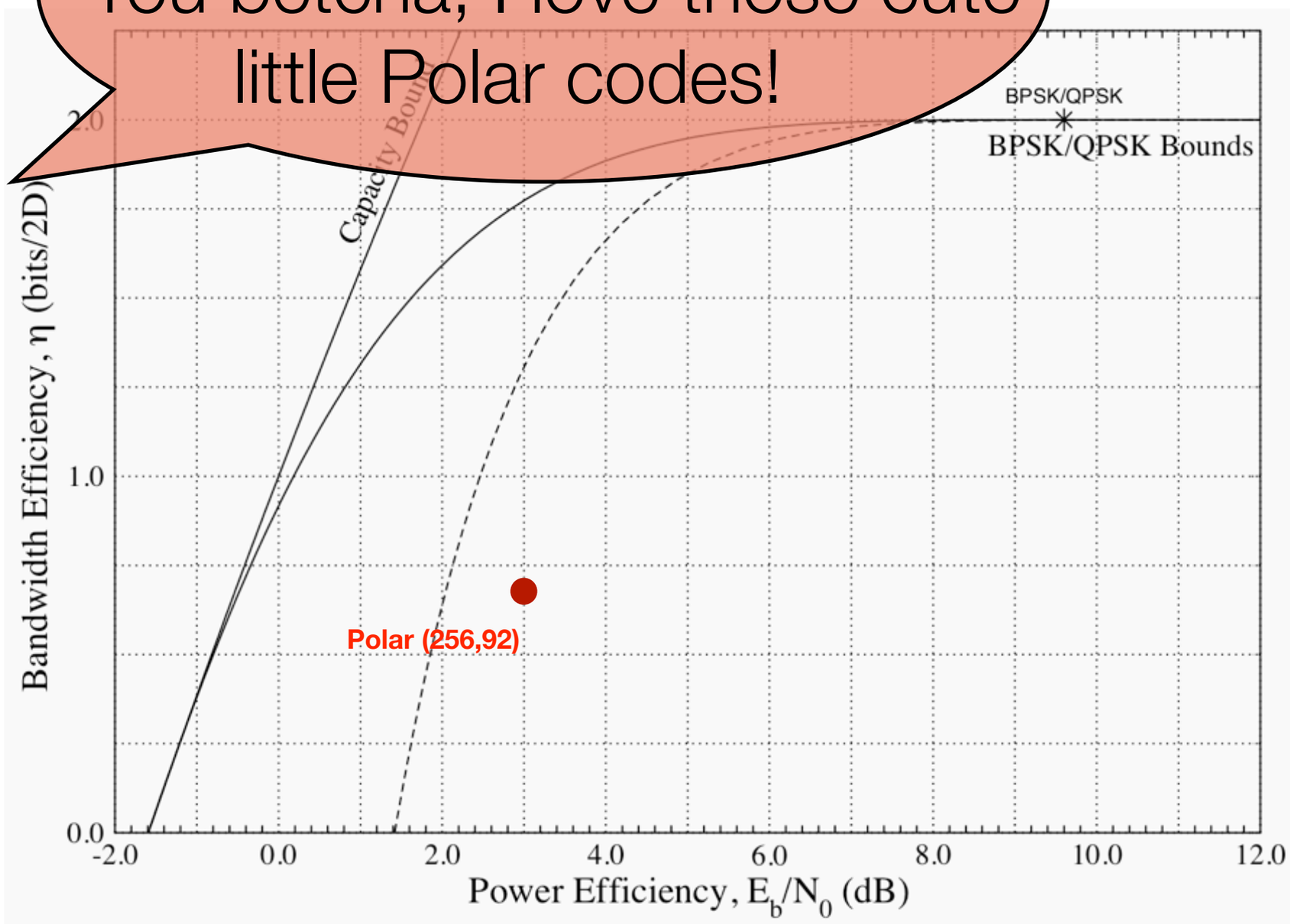
Sarah Palin - *US Vice-Presidential Candidate (2008)*



Political Views on Coding Theory

Sarah Palin - *US Vice-Presidential Candidate (2008)*

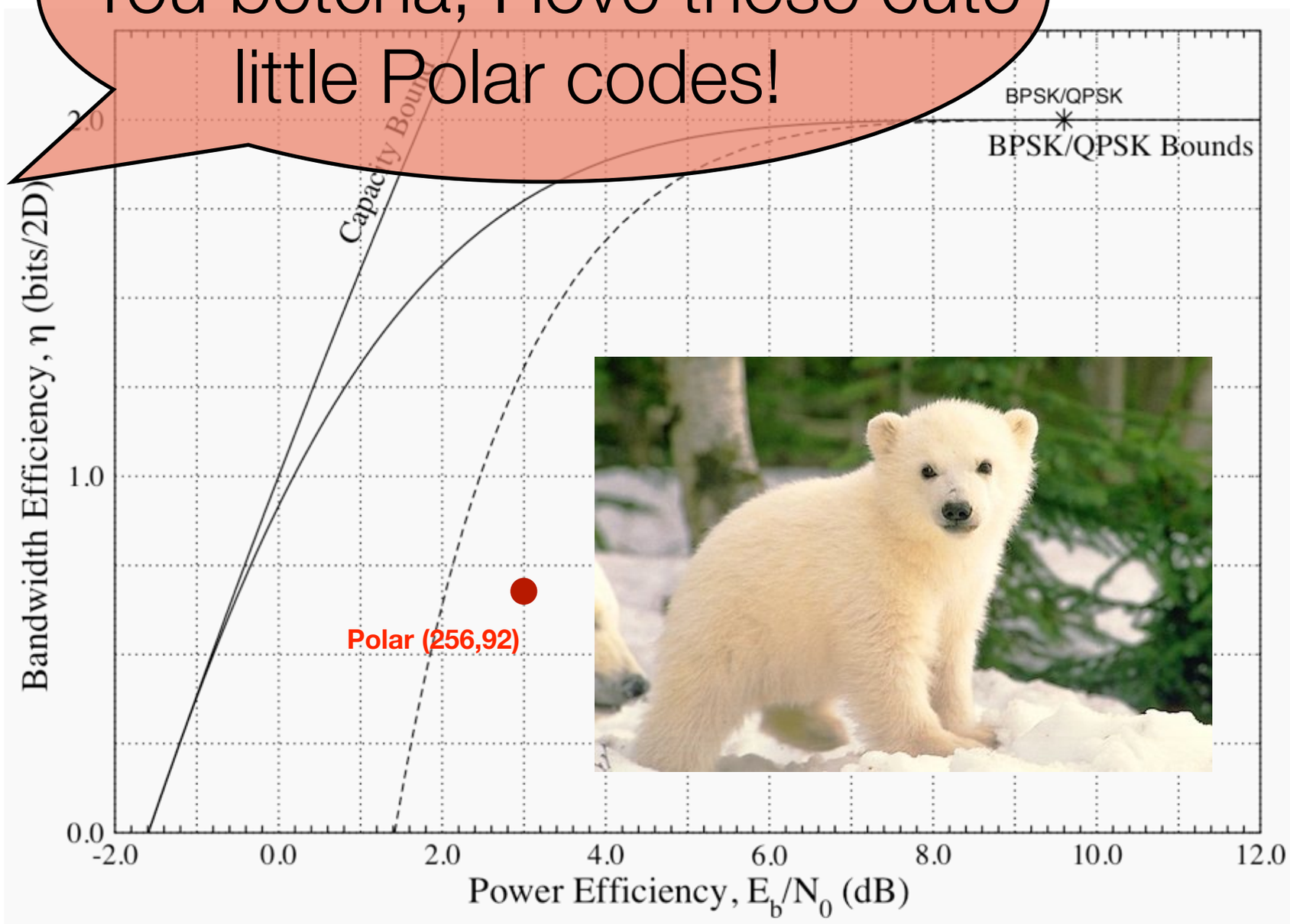
I'm from Alaska.
You betcha, I love those cute little Polar codes!



Political Views on Coding Theory

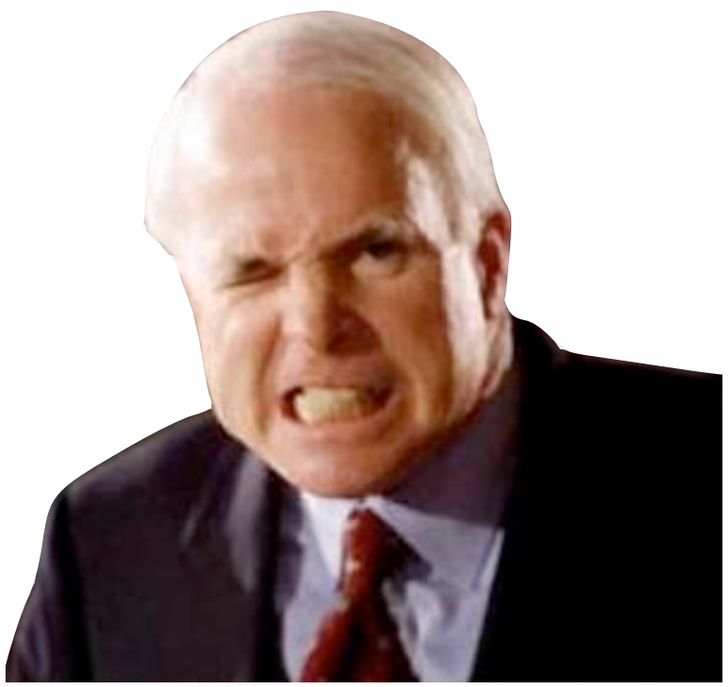
Sarah Palin - *US Vice-Presidential Candidate (2008)*

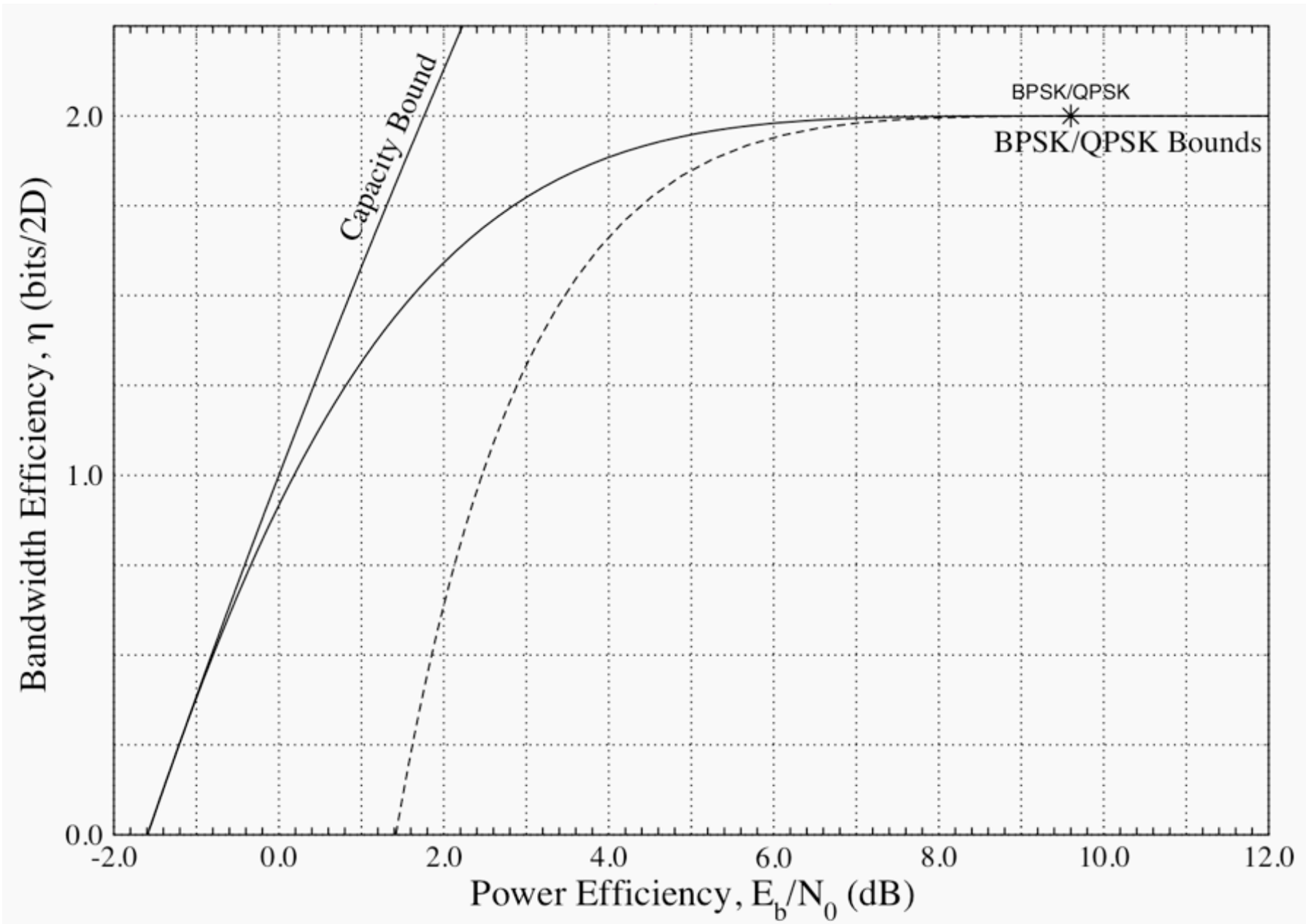
I'm from Alaska.
You betcha, I love those cute little Polar codes!



Political Views on Coding Theory

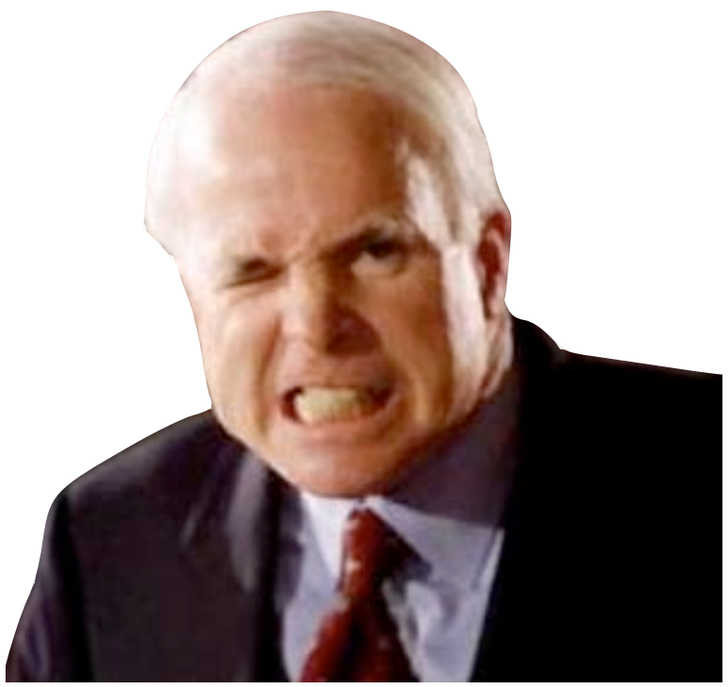
John McCain - *US Presidential Candidate (2000, 2008)*

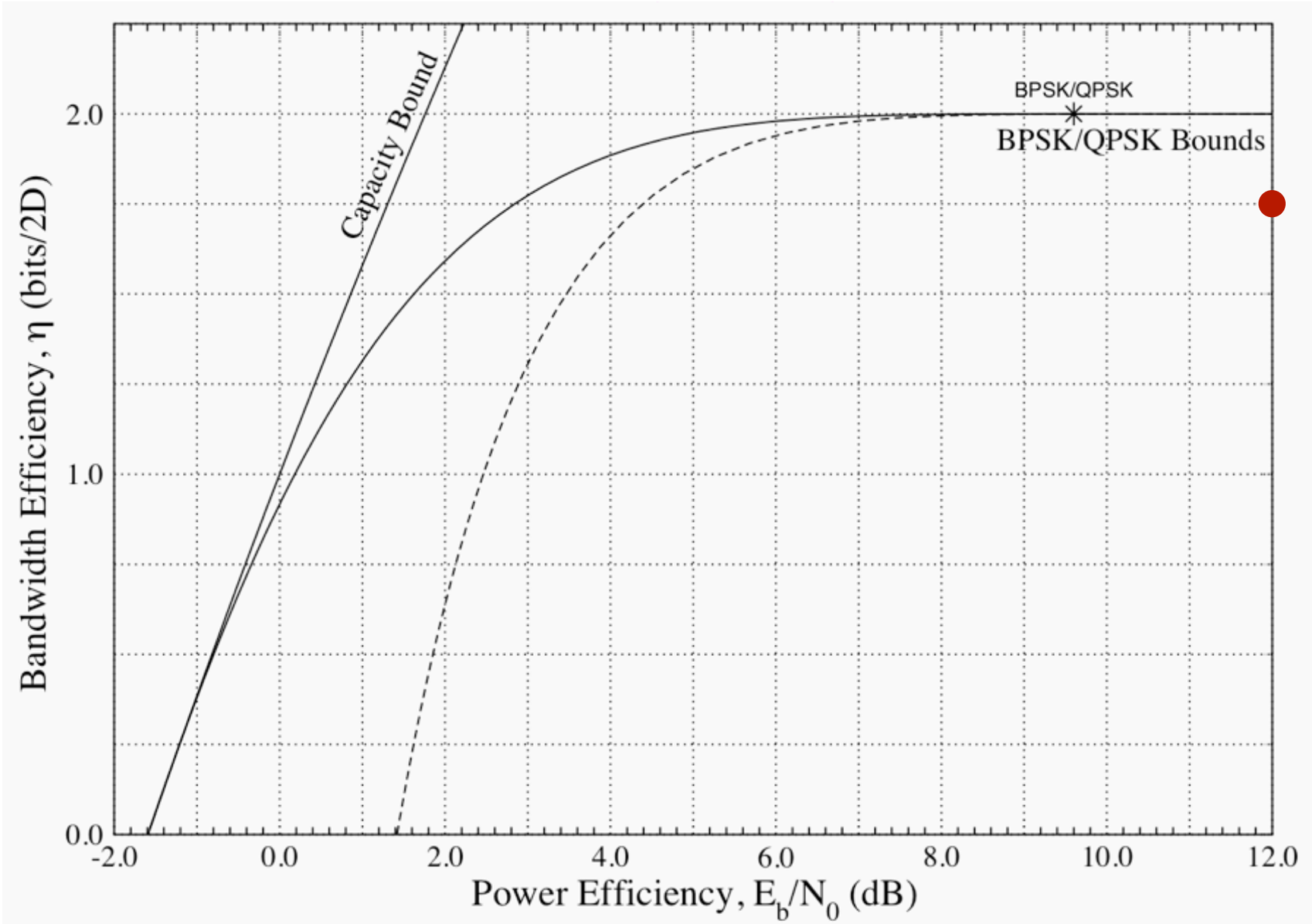




Political Views on Coding Theory

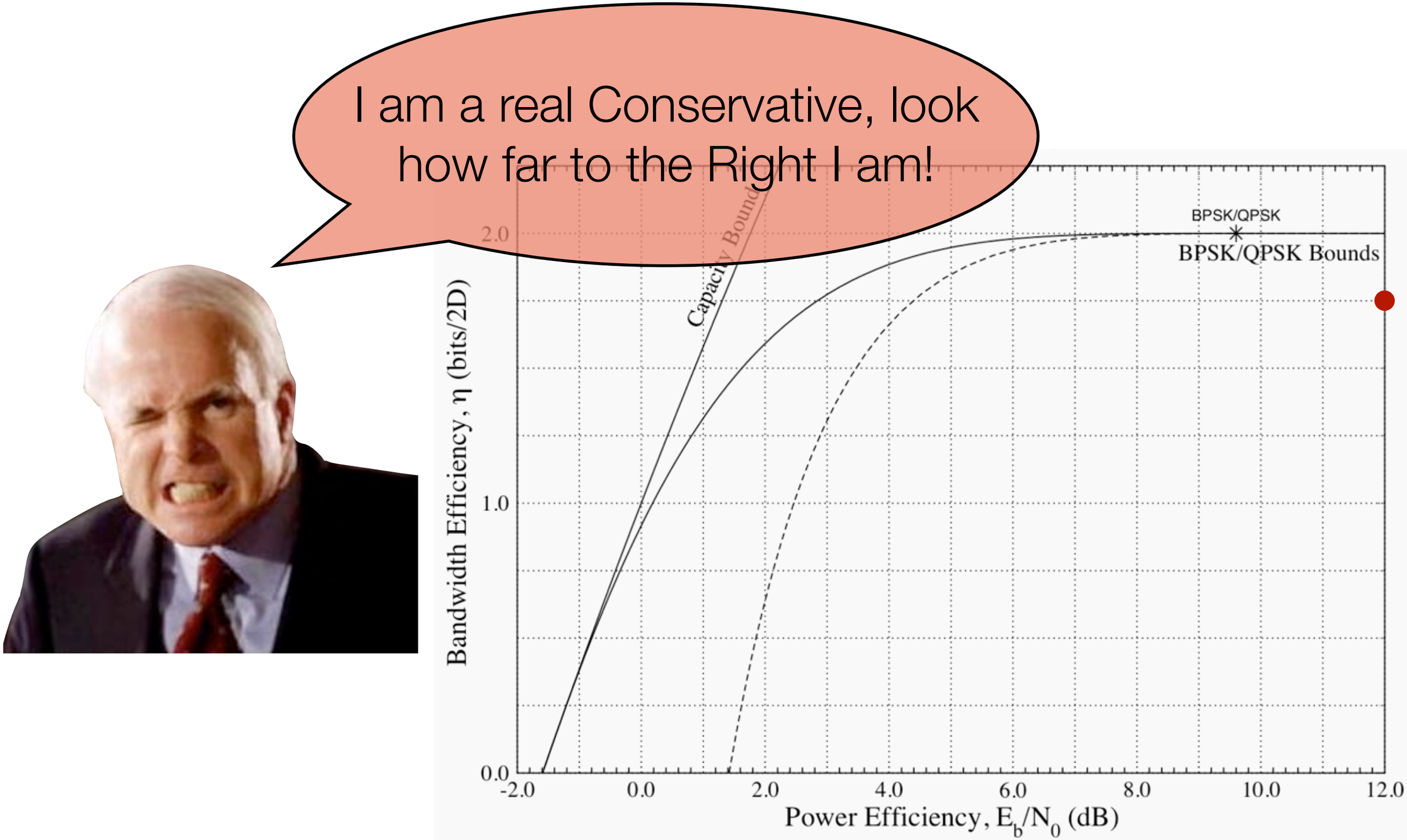
John McCain - *US Presidential Candidate (2000, 2008)*





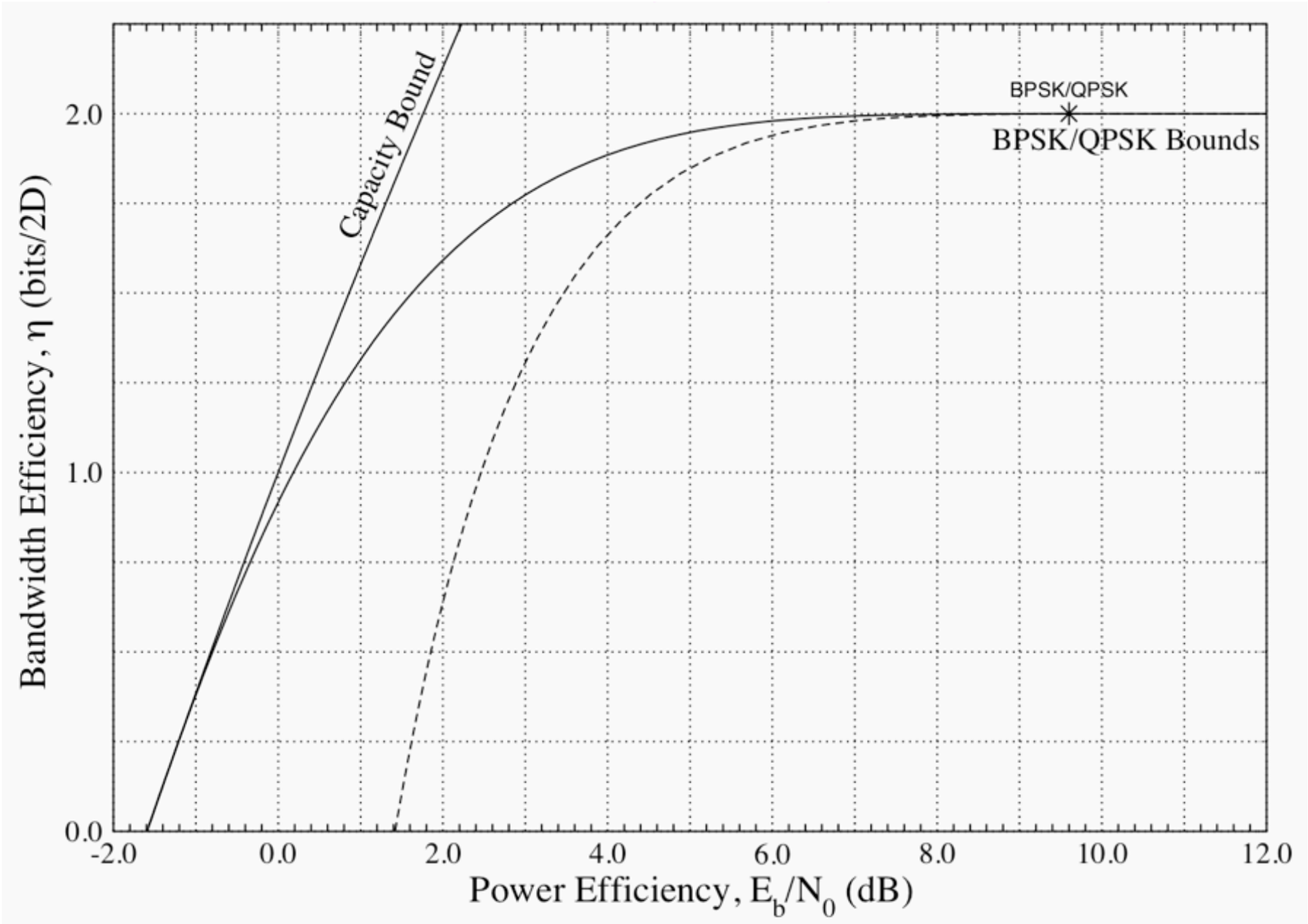
Political Views on Coding Theory

John McCain - *US Presidential Candidate (2000, 2008)*



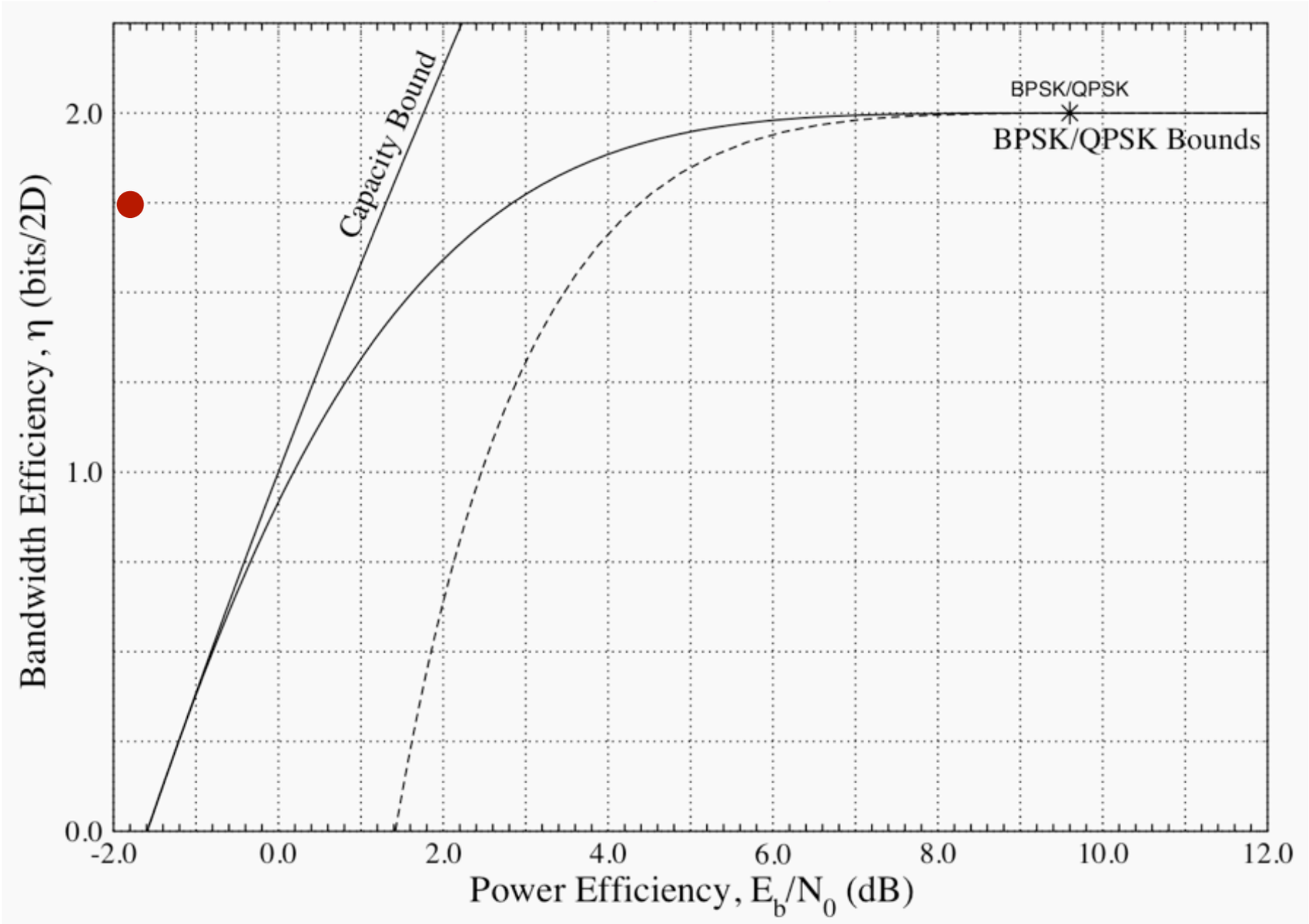
Political Views on Coding Theory

Barack Obama - *US President (2008-2016)*



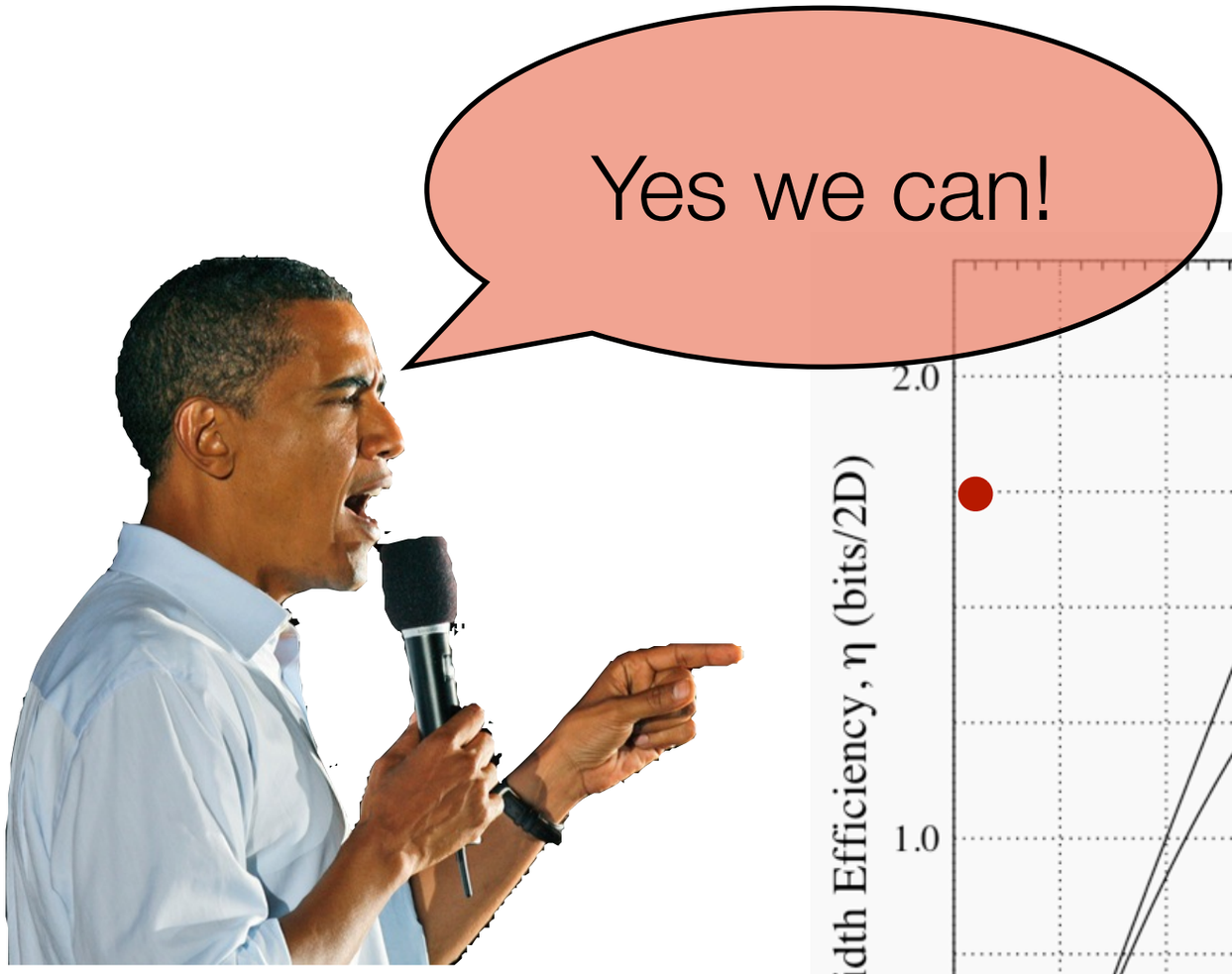
Political Views on Coding Theory

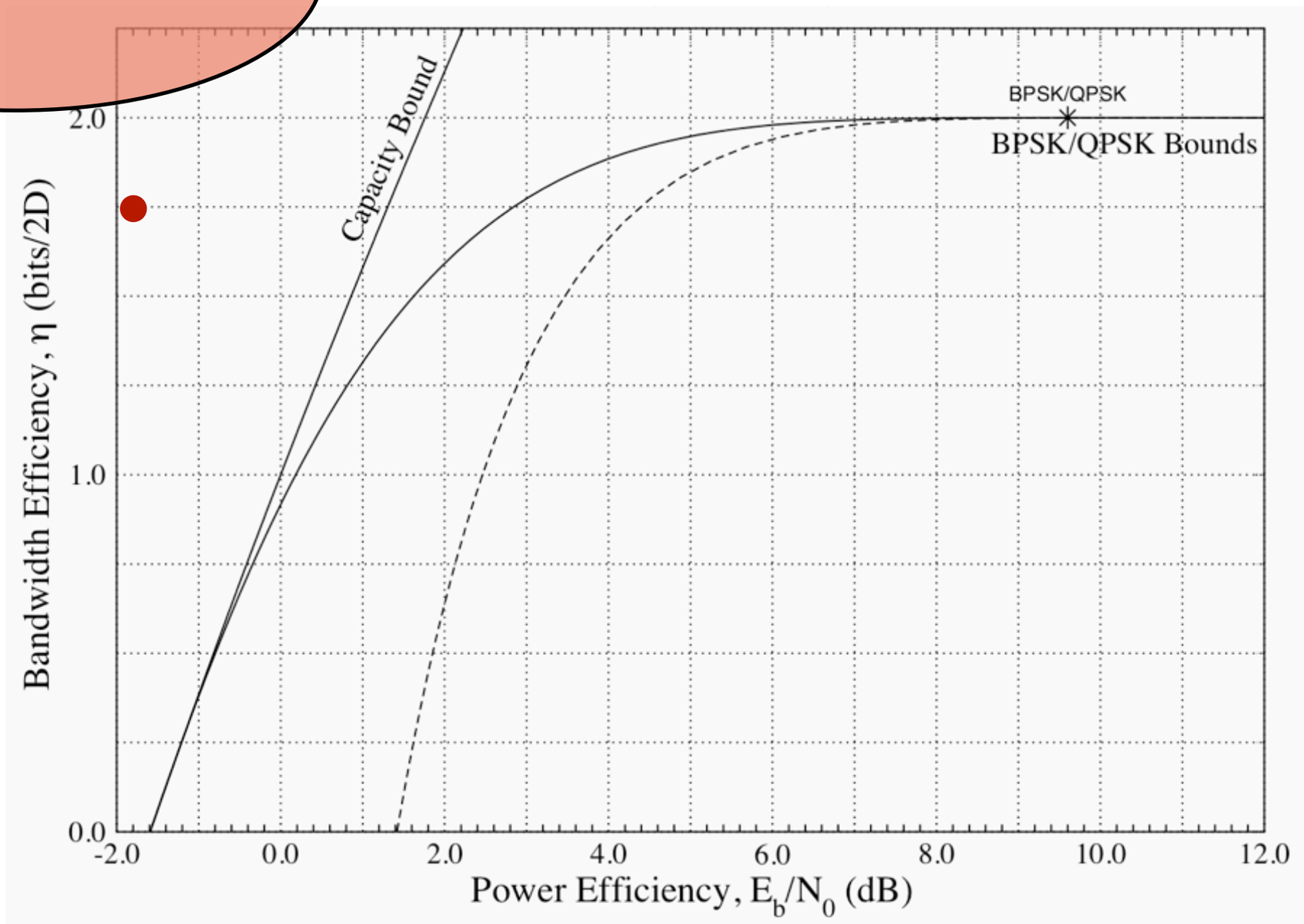
Barack Obama - *US President (2008-2016)*



Political Views on Coding Theory

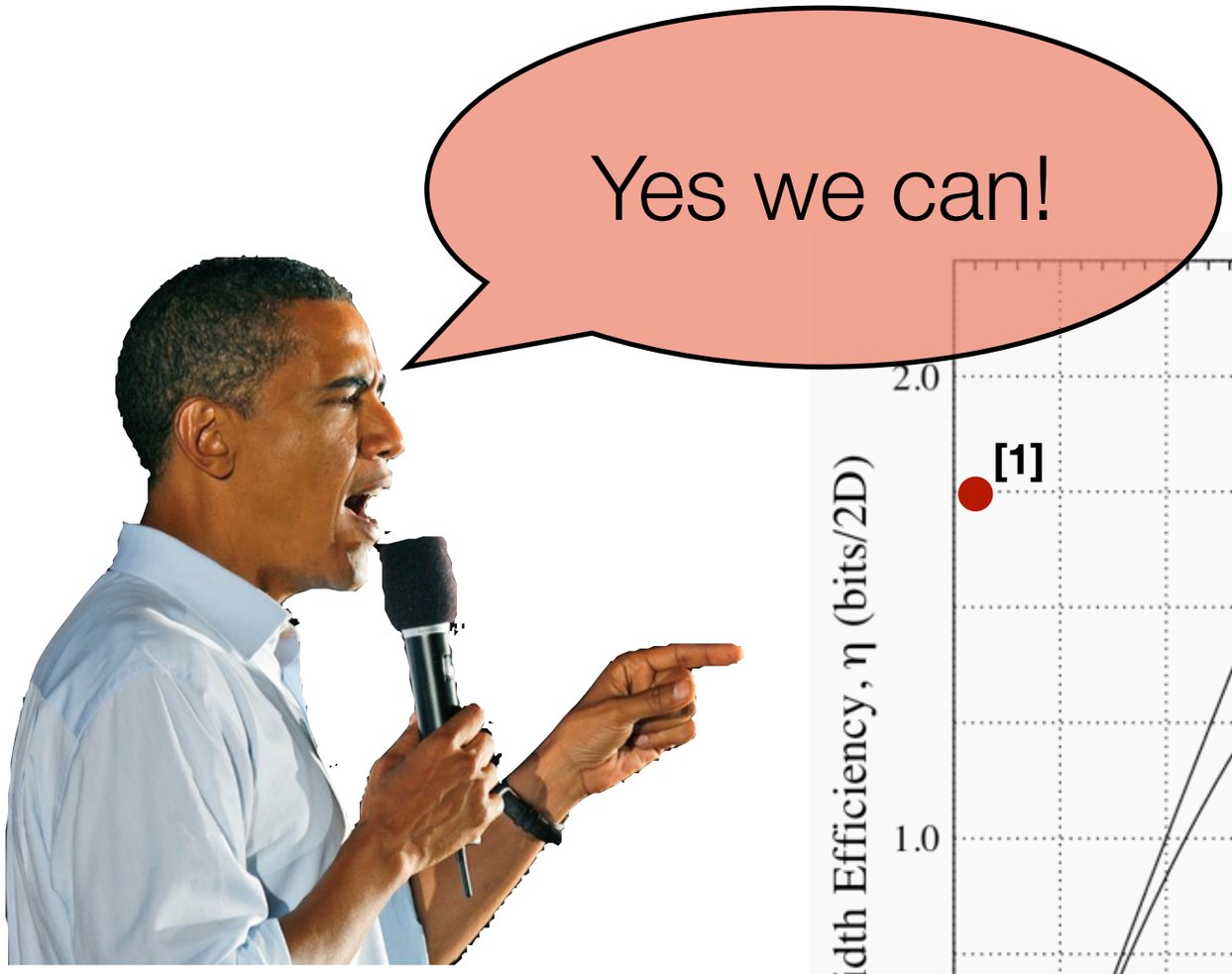
Barack Obama - *US President (2008-2016)*

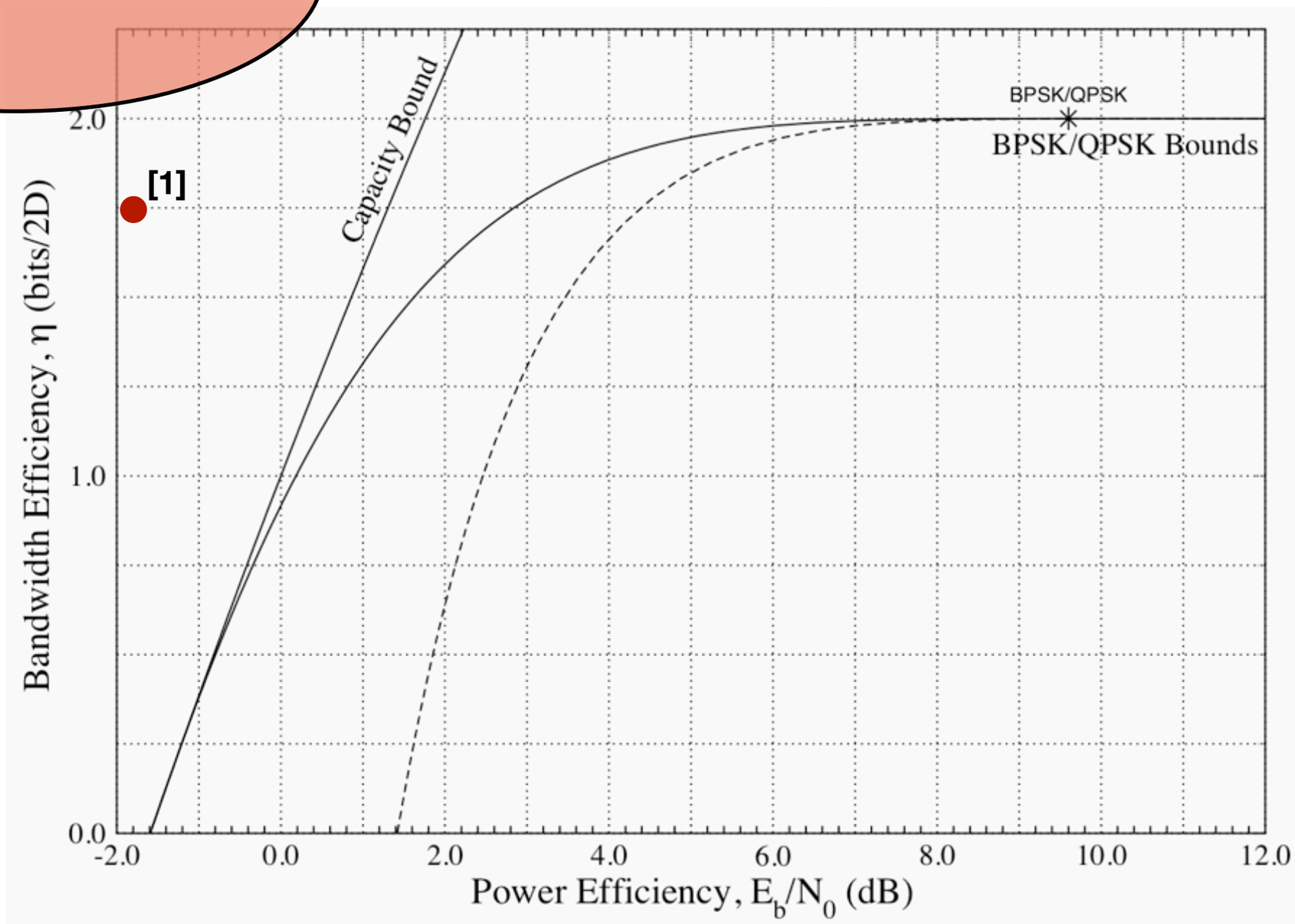




Political Views on Coding Theory

Barack Obama - *US President (2008-2016)*

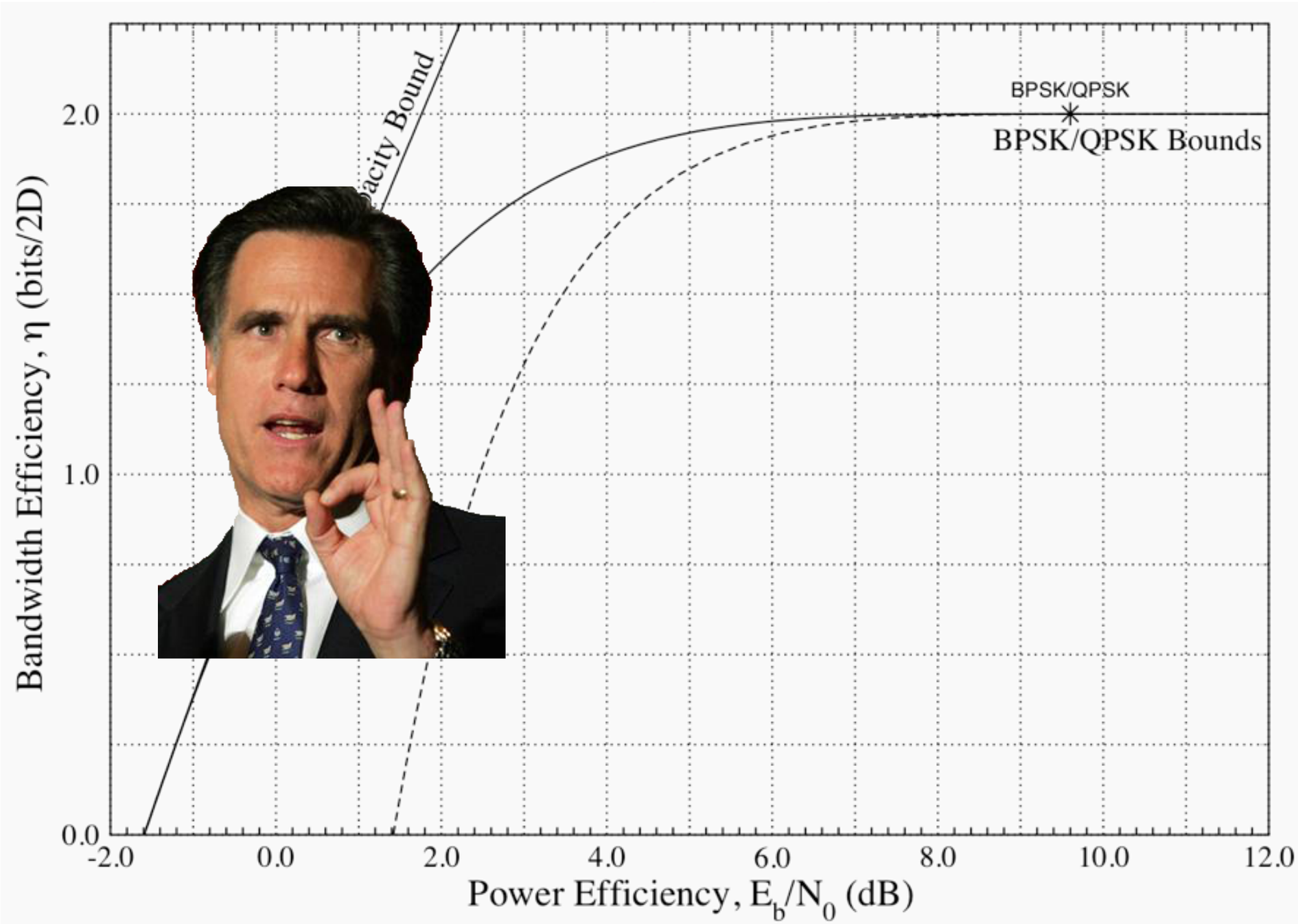




[1] B. H. Obama, "The audacity of hope," Three Rivers Press, New York, NY, 2007.

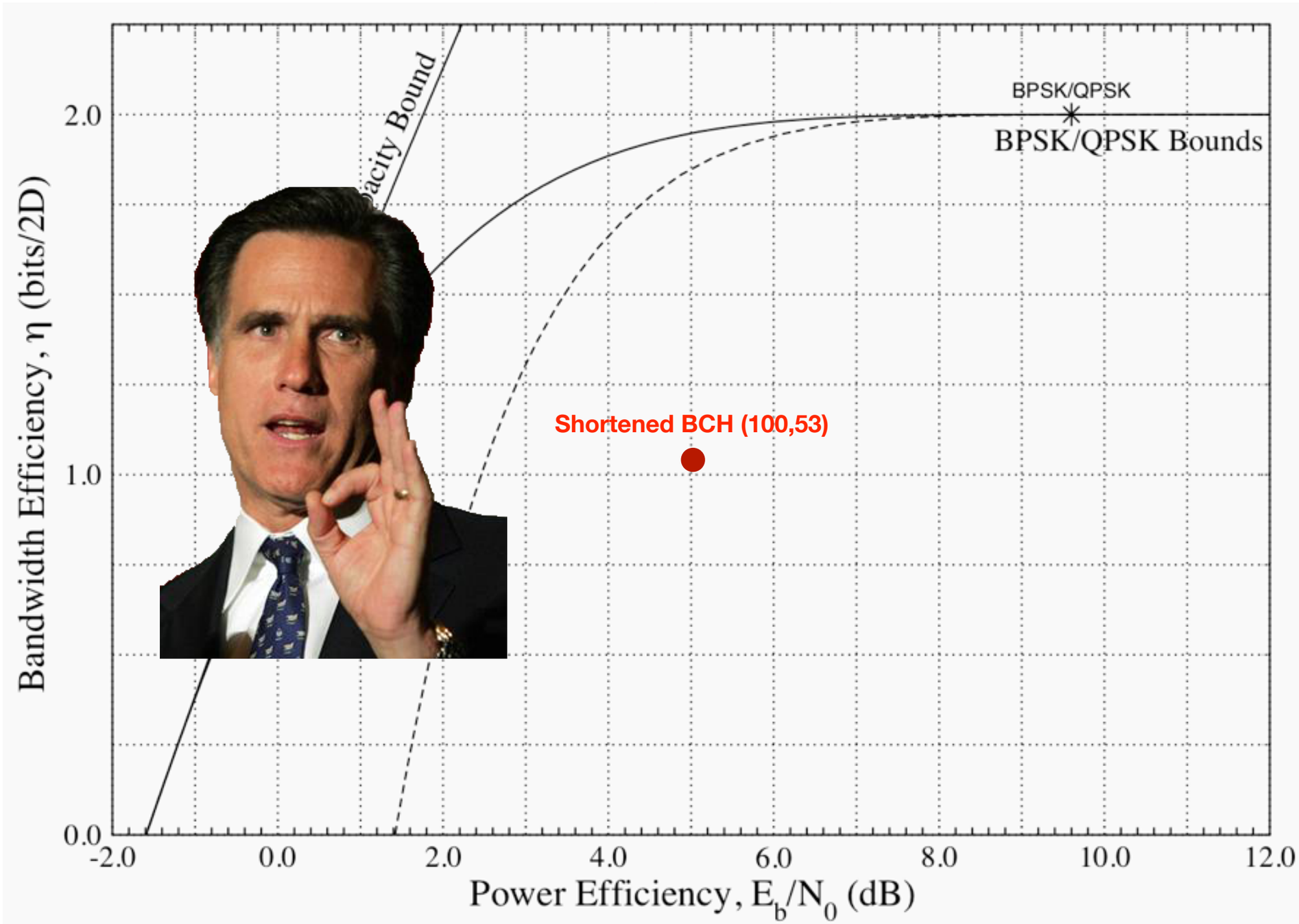
Political Views on Coding Theory

Mitt Romney - *US Presidential Candidate (2012)*



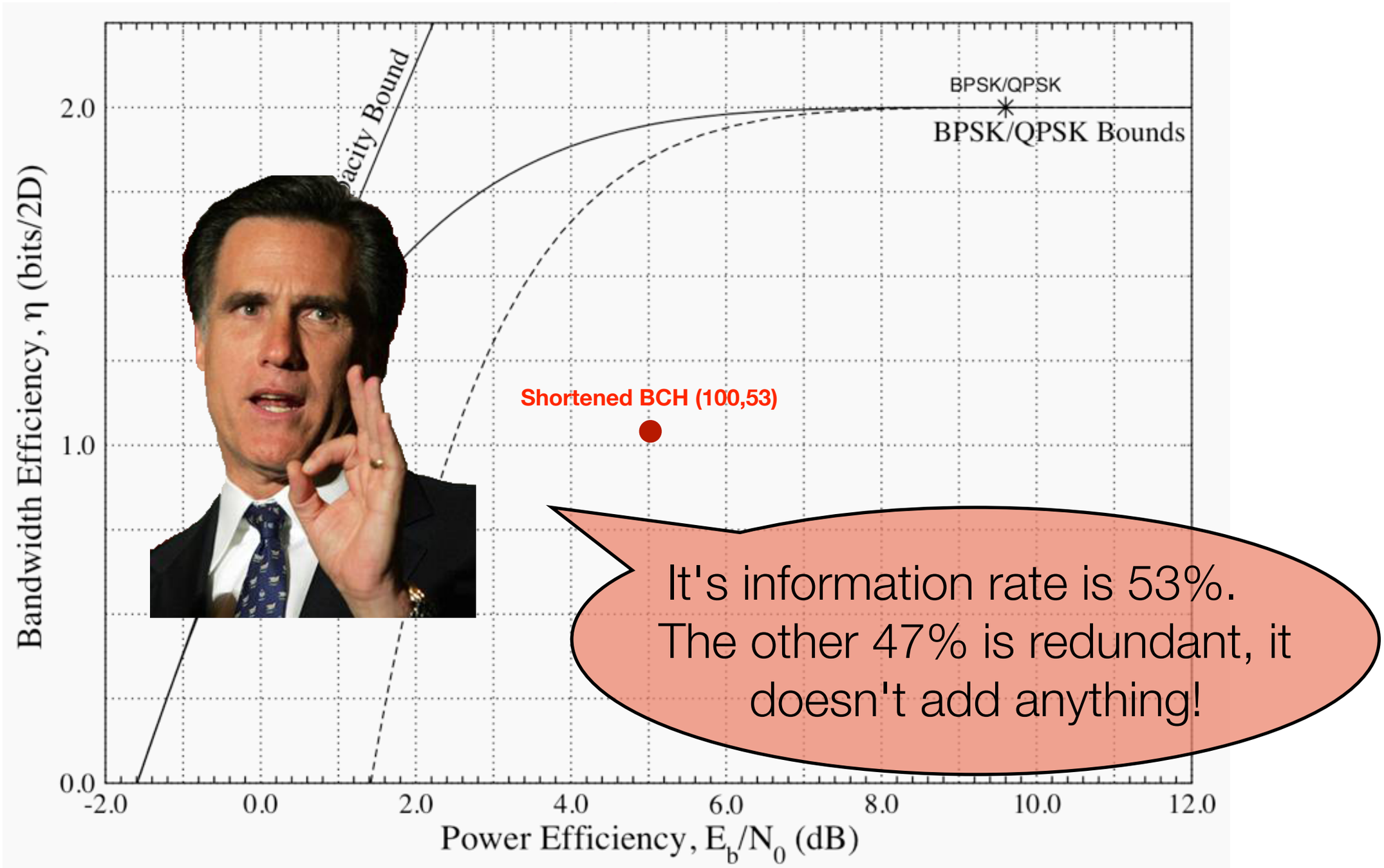
Political Views on Coding Theory

Mitt Romney - *US Presidential Candidate (2012)*



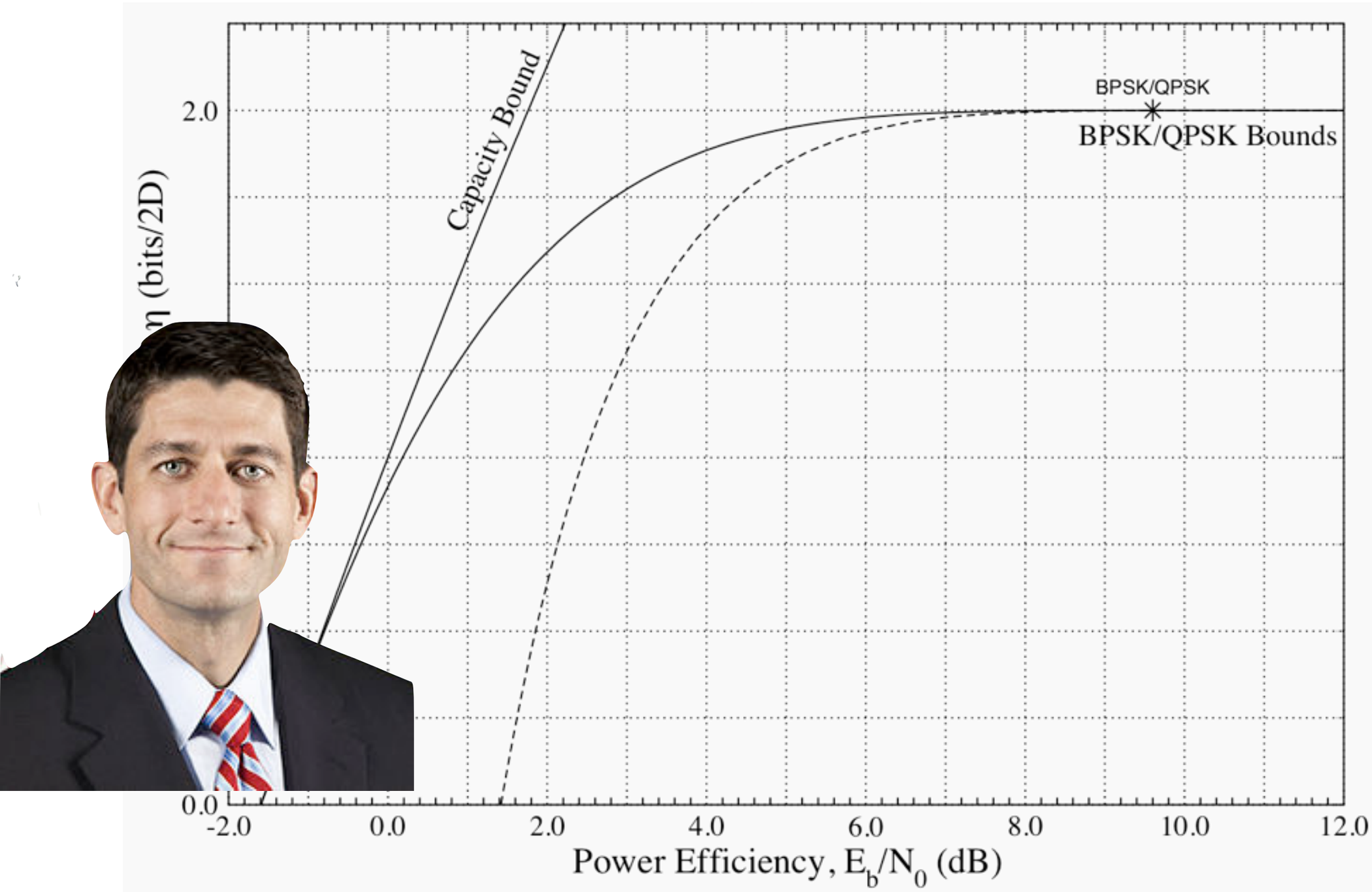
Political Views on Coding Theory

Mitt Romney - *US Presidential Candidate (2012)*



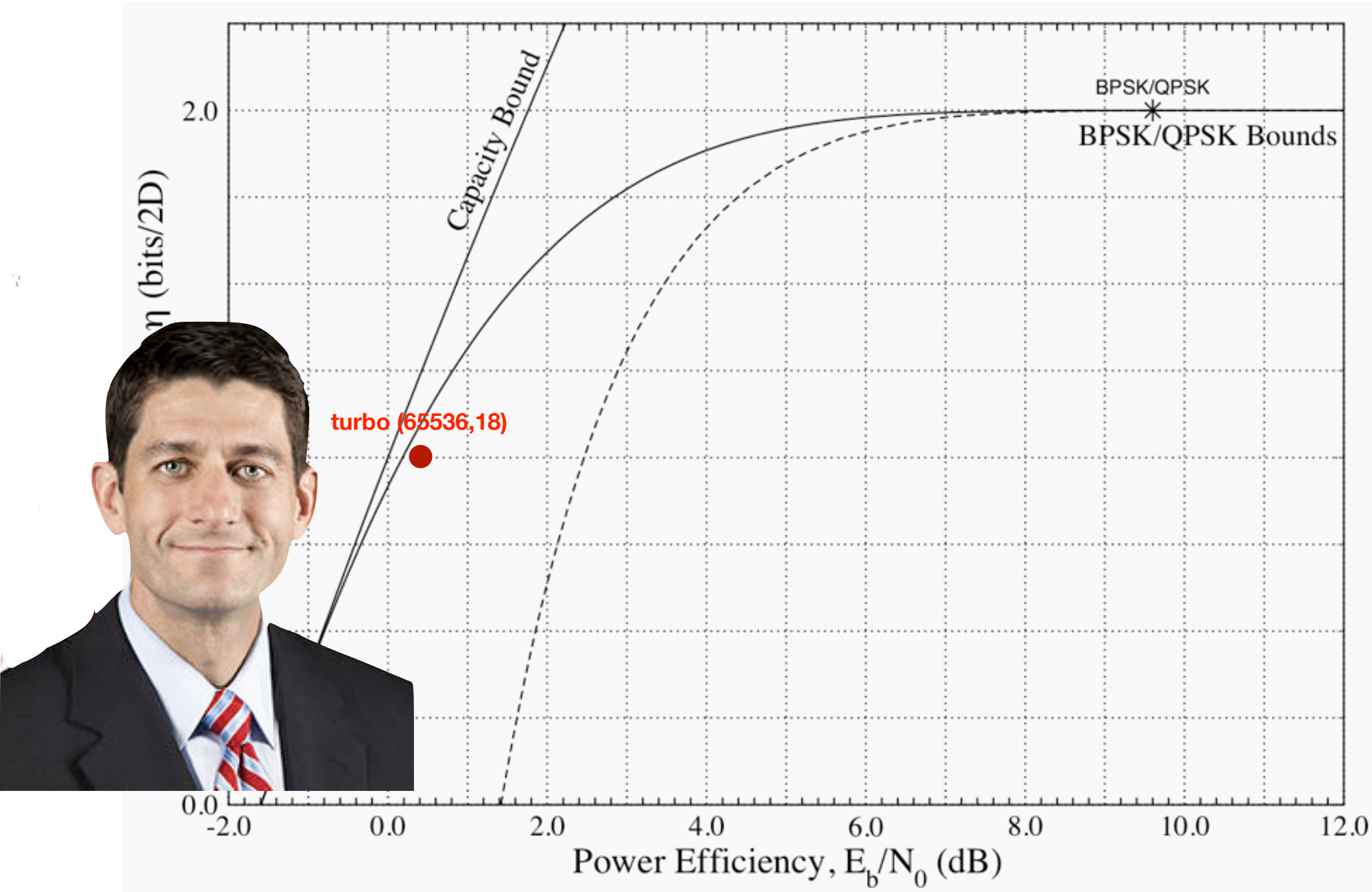
Political Views on Coding Theory

Paul Ryan - *US Vice-Presidential Candidate (2012)*



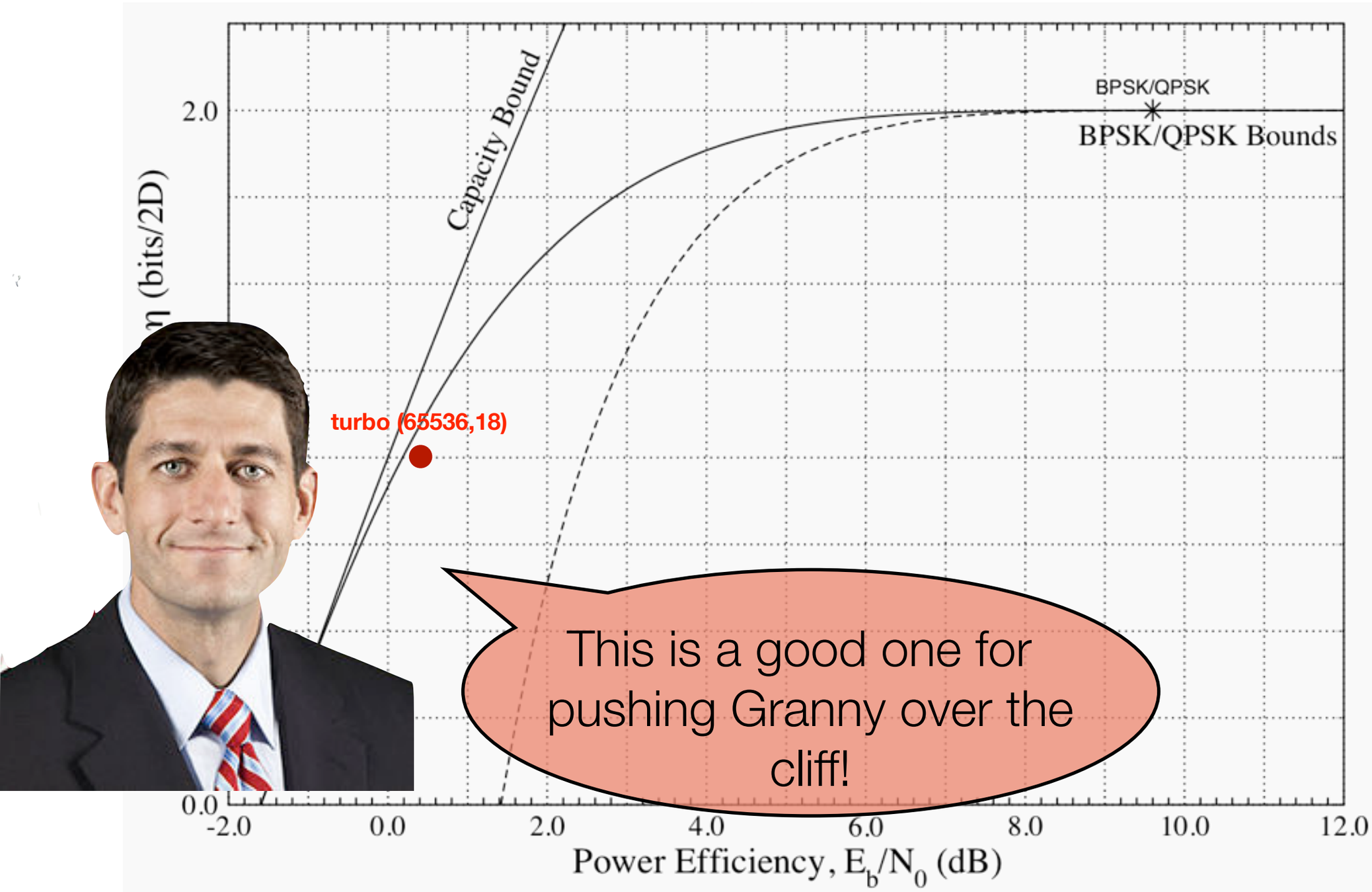
Political Views on Coding Theory

Paul Ryan - *US Vice-Presidential Candidate (2012)*



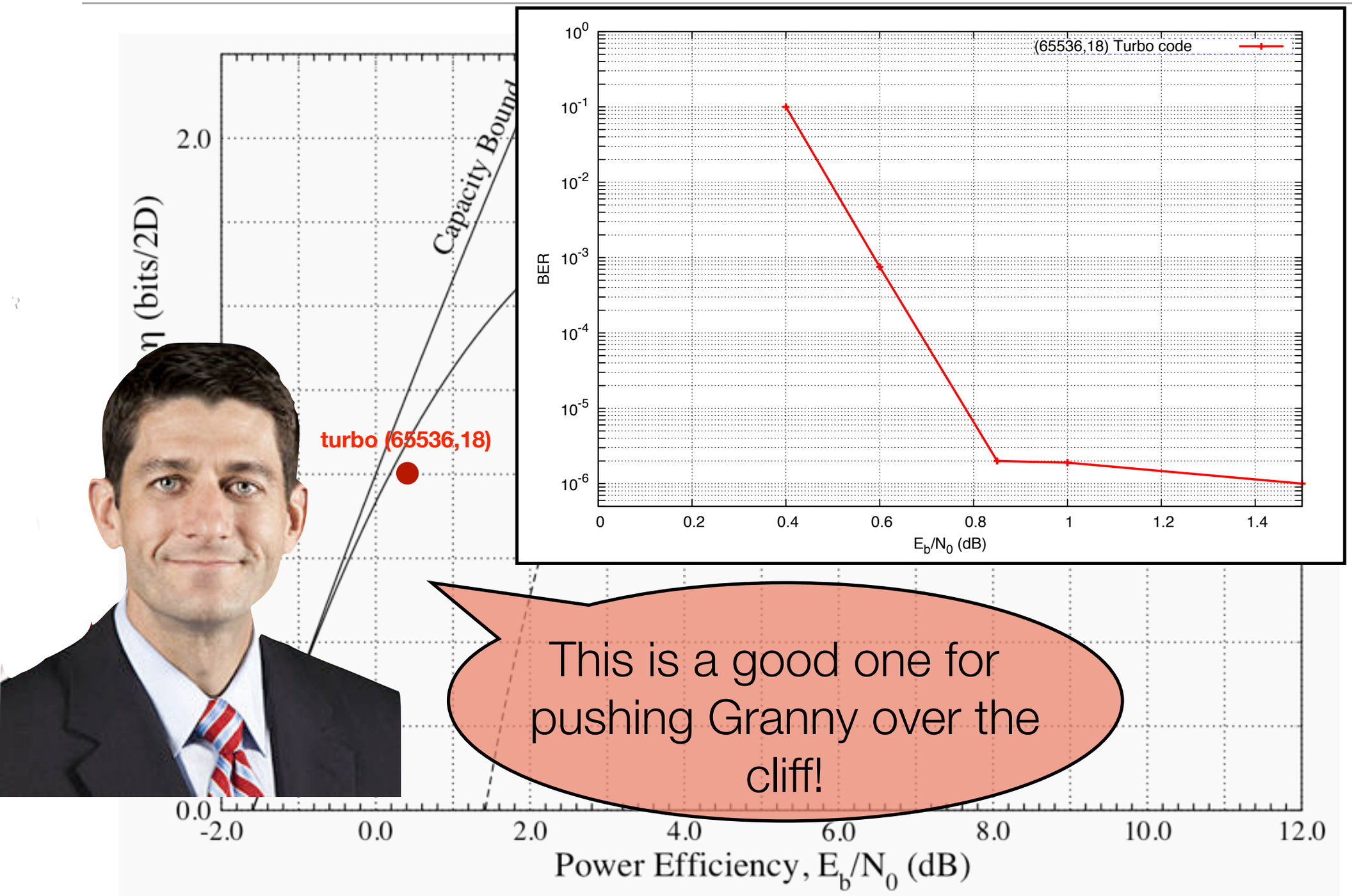
Political Views on Coding Theory

Paul Ryan - *US Vice-Presidential Candidate (2012)*



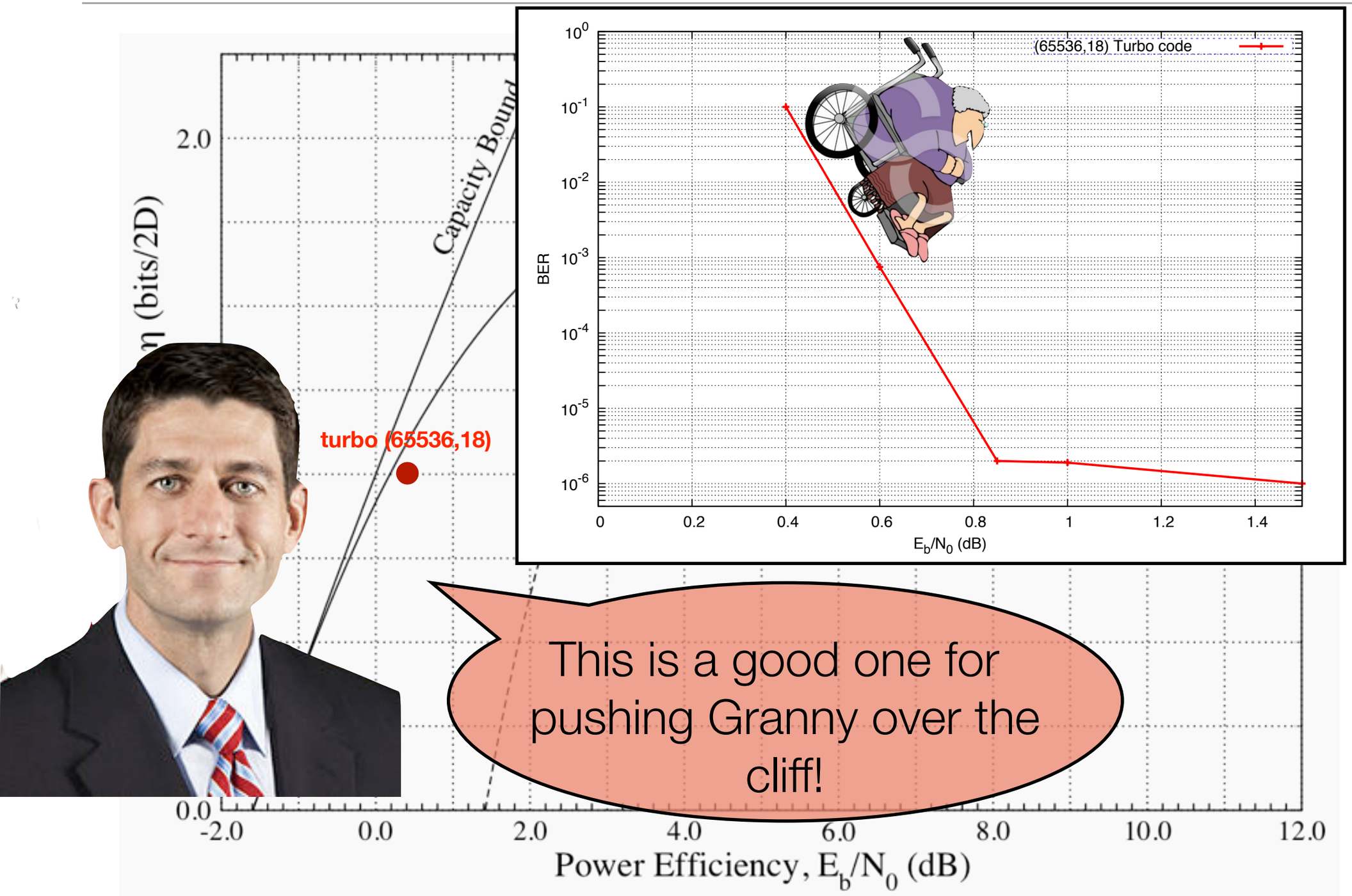
Political Views on Coding Theory

Paul Ryan - *US Vice-Presidential Candidate (2012)*



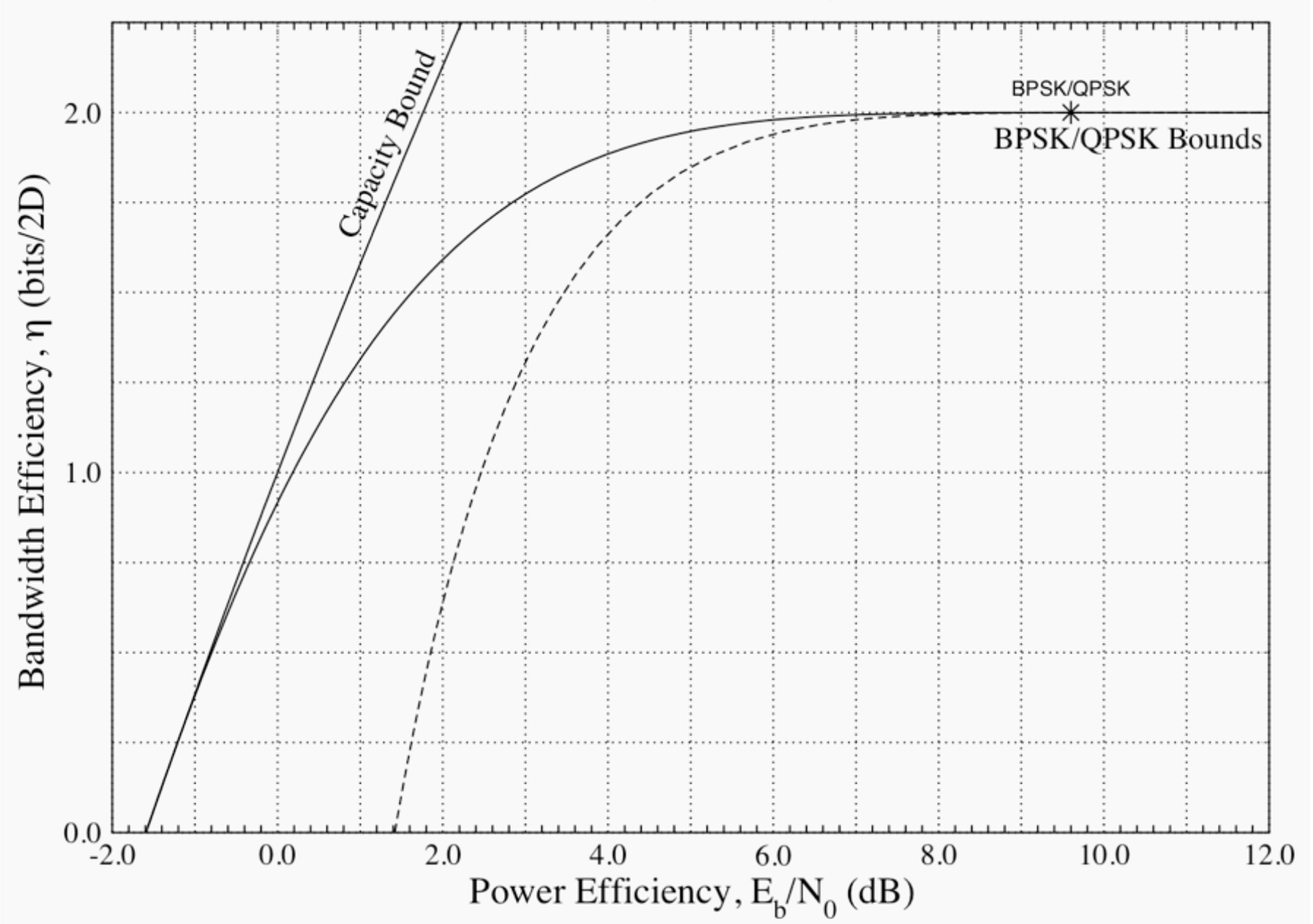
Political Views on Coding Theory

Paul Ryan - *US Vice-Presidential Candidate (2012)*



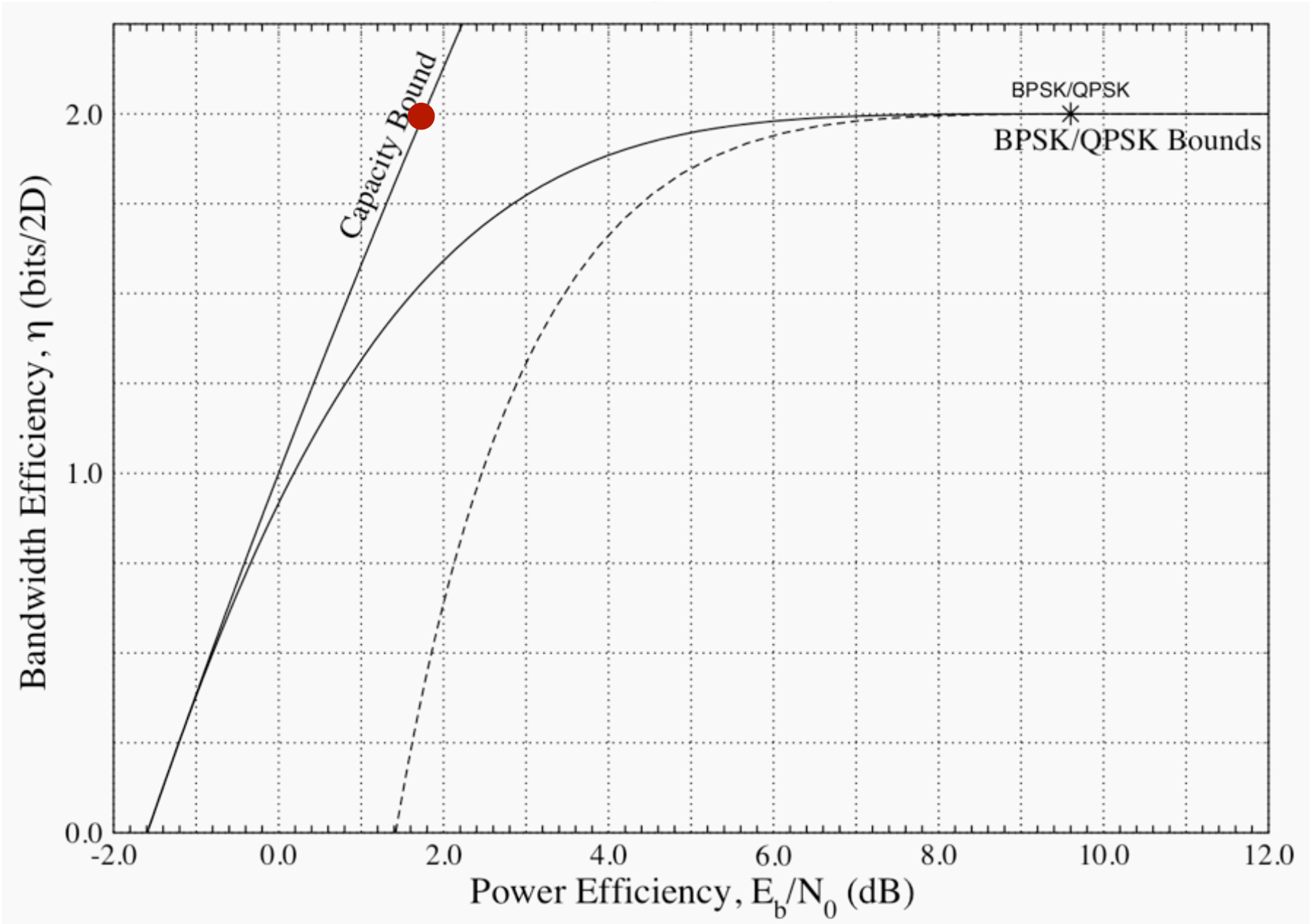
Political Views on Coding Theory

Edward Snowden



Political Views on Coding Theory

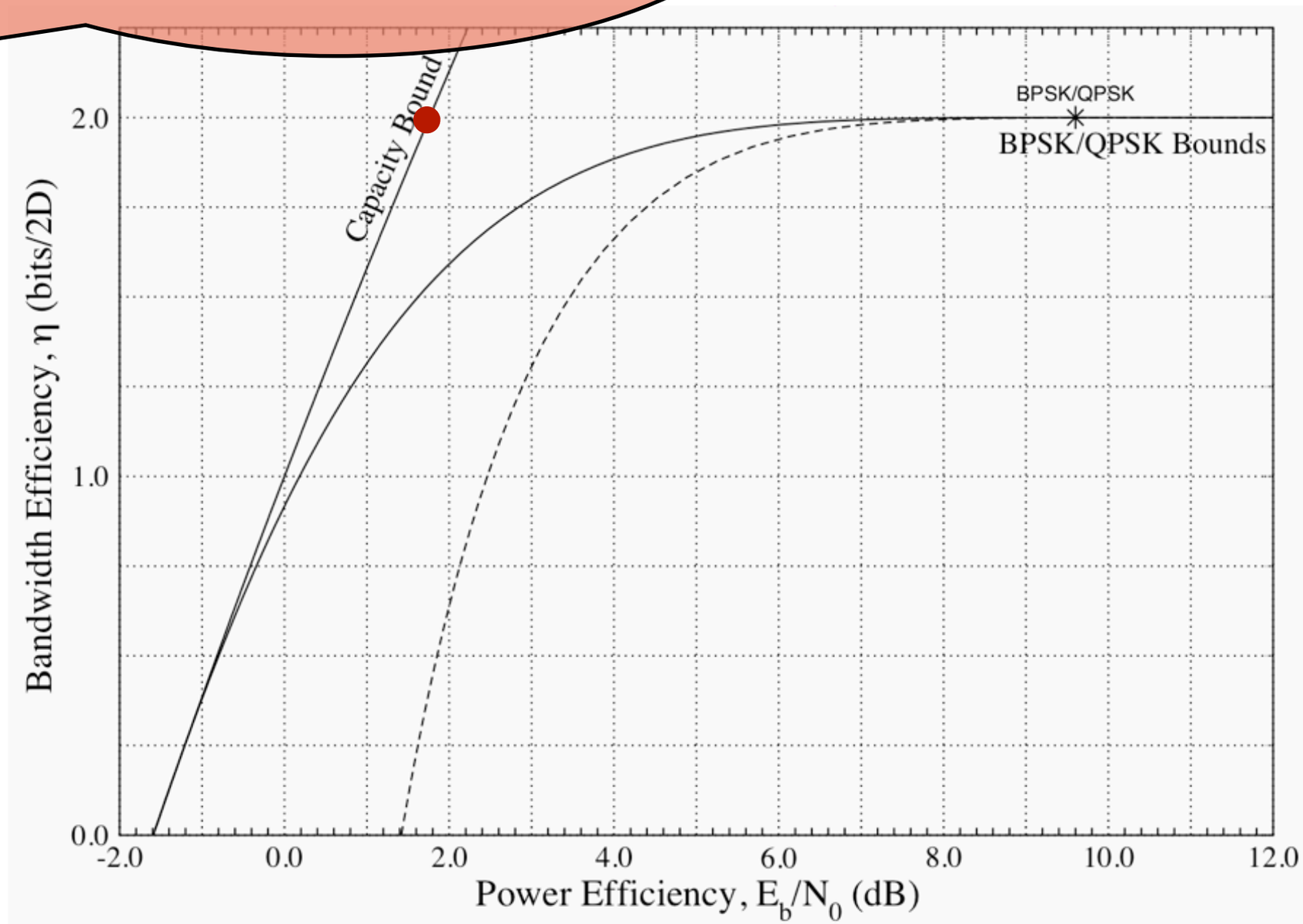
Edward Snowden



Political Views on Coding Theory

Edward Snowden

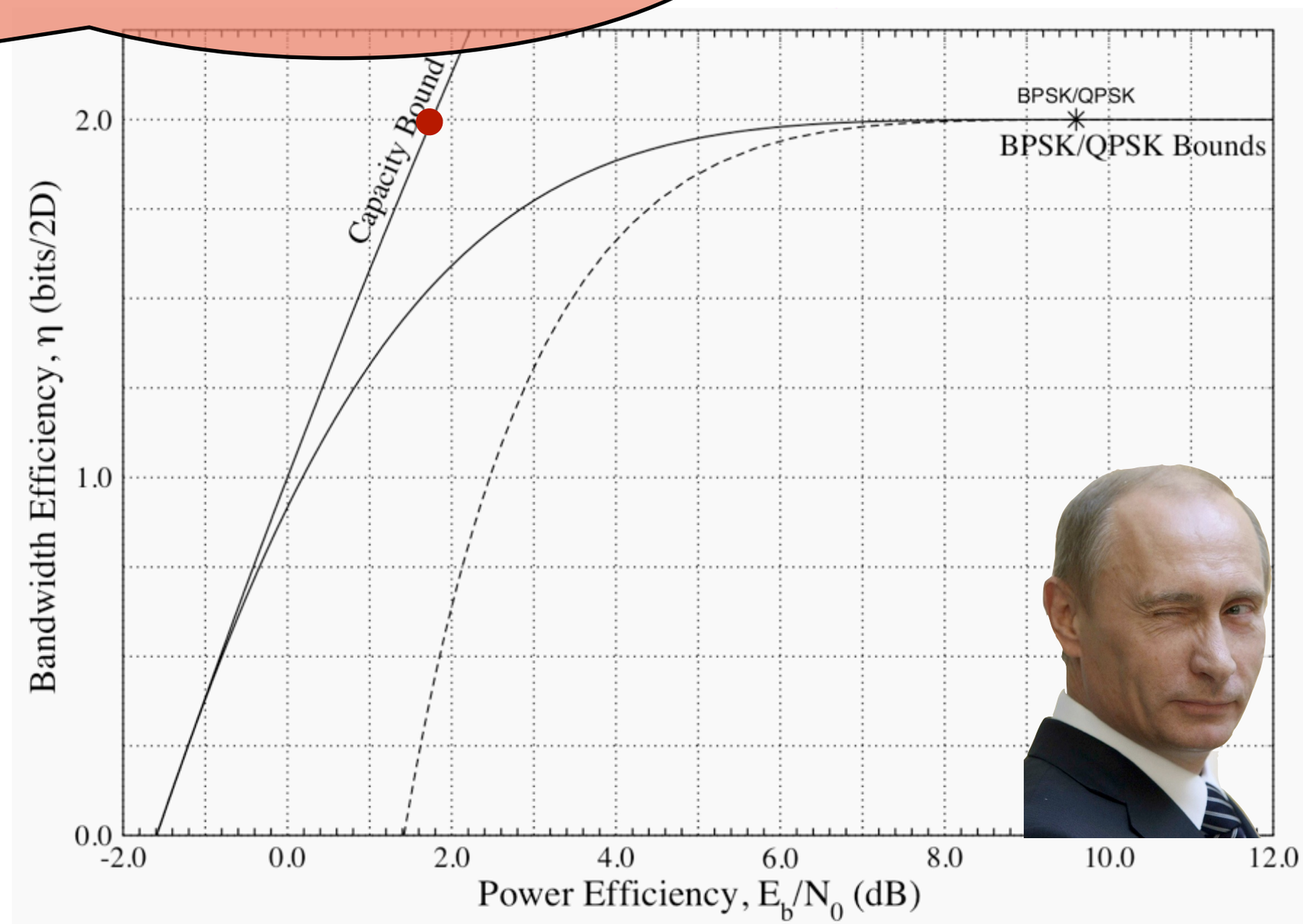
I can't tell you, it's a government secret!



Political Views on Coding Theory

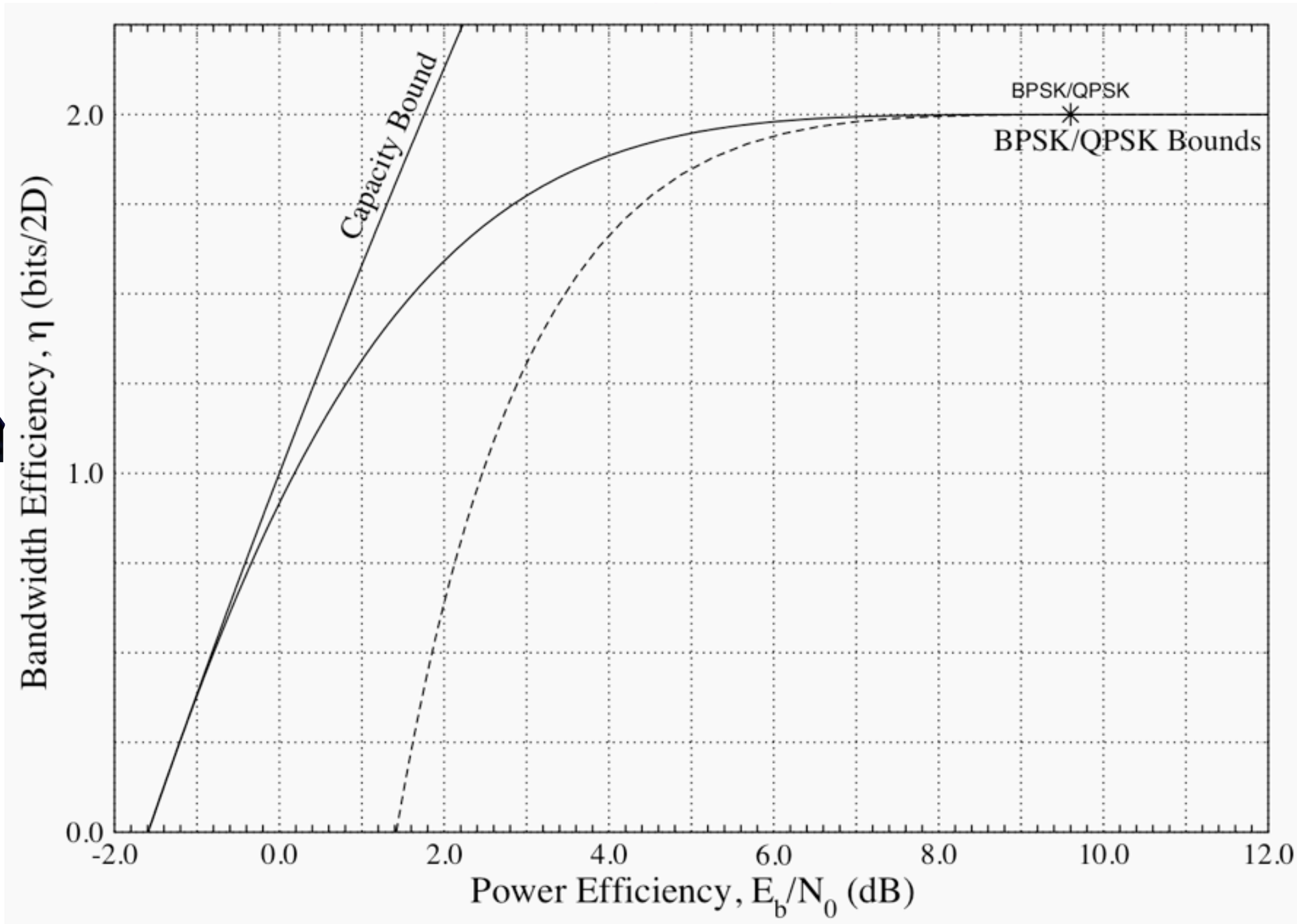
Edward Snowden

I can't tell you, it's a government secret!



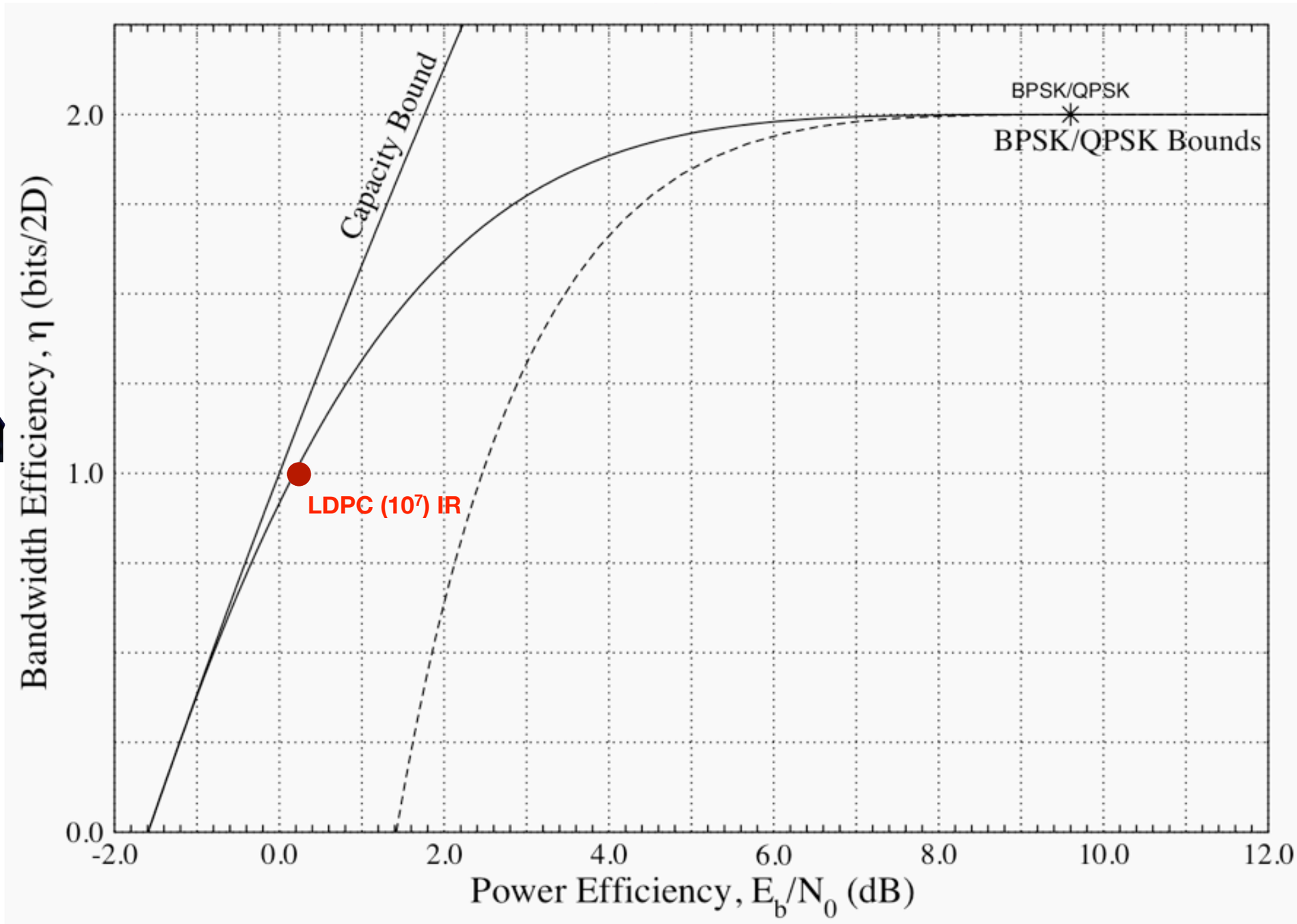
Political Views on Coding Theory

Hillary Clinton - *US Presidential Candidate (2008+4k, k=0,1,...)*



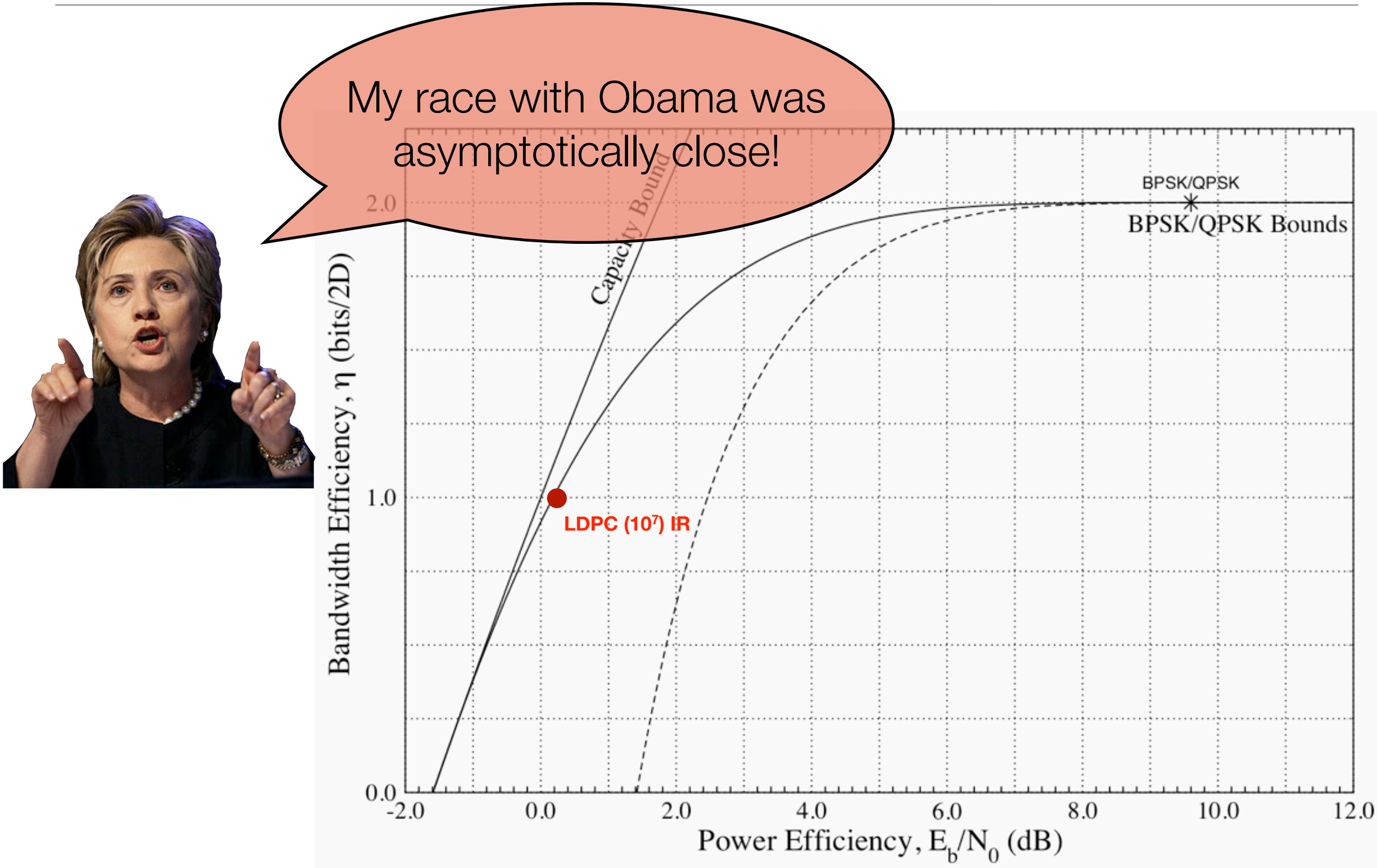
Political Views on Coding Theory

Hillary Clinton - *US Presidential Candidate (2008+4k, k=0,1,...)*



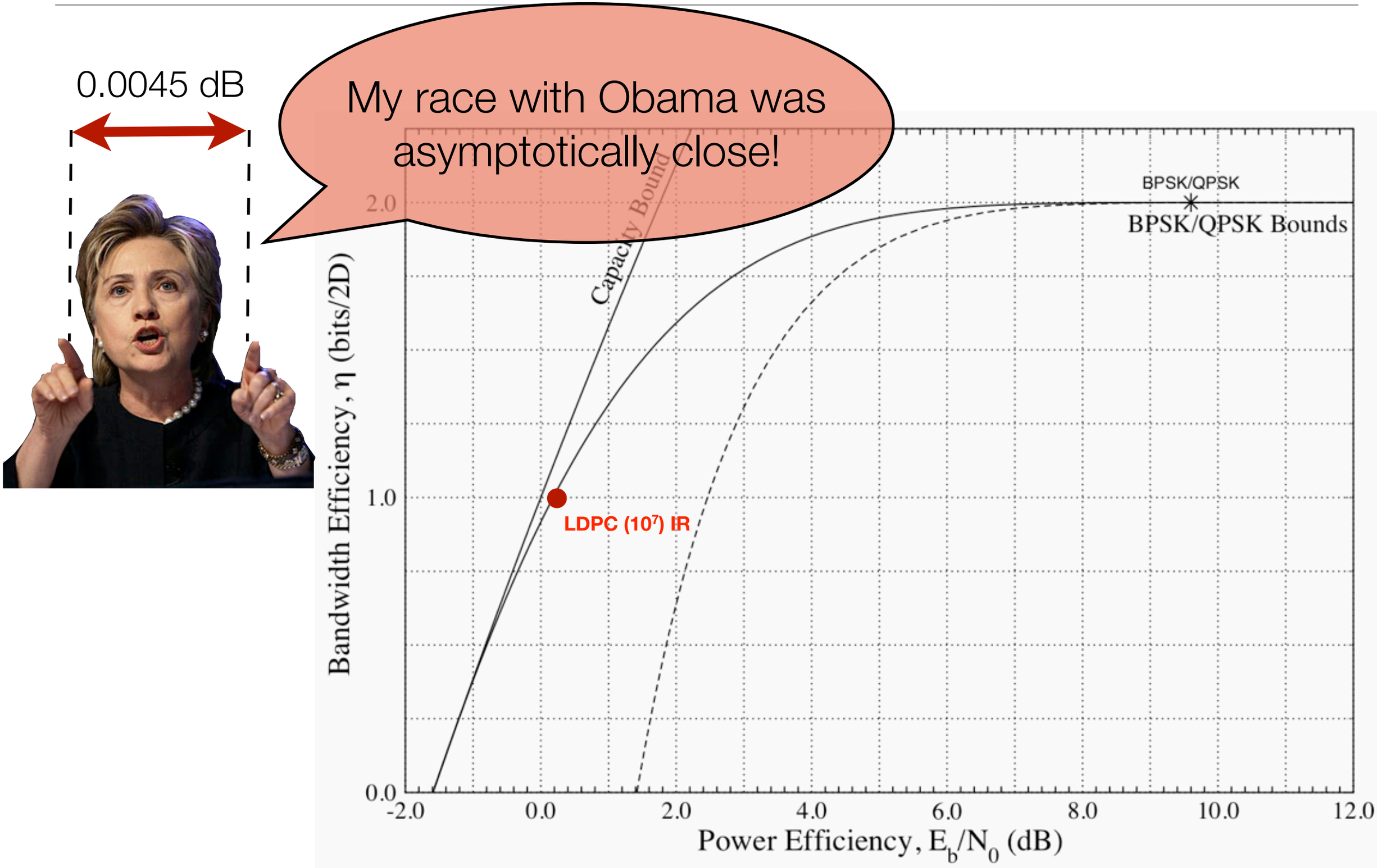
Political Views on Coding Theory

Hillary Clinton - *US Presidential Candidate (2008+4k, k=0,1,...)*



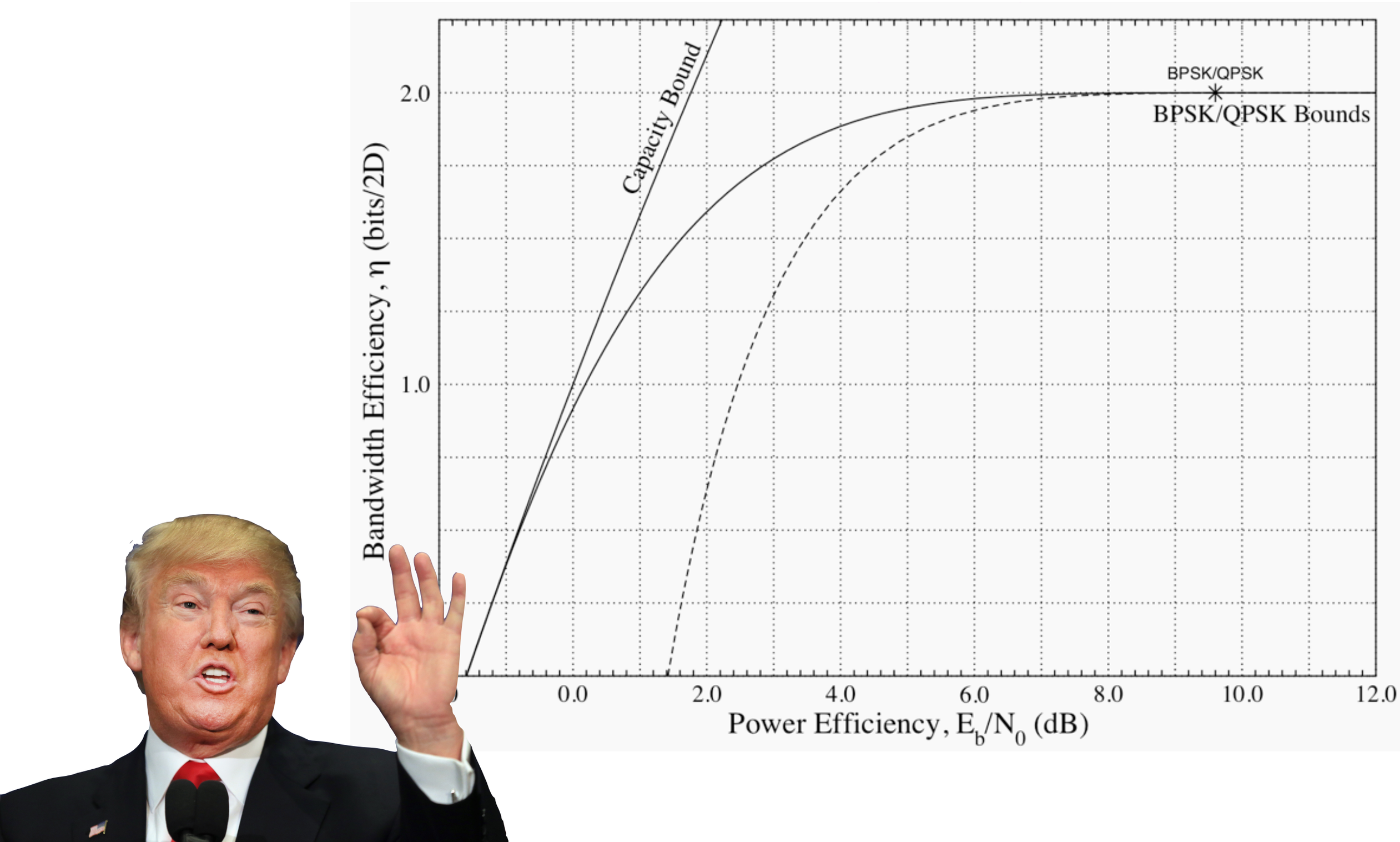
Political Views on Coding Theory

Hillary Clinton - *US Presidential Candidate (2008+4k, k=0,1,...)*



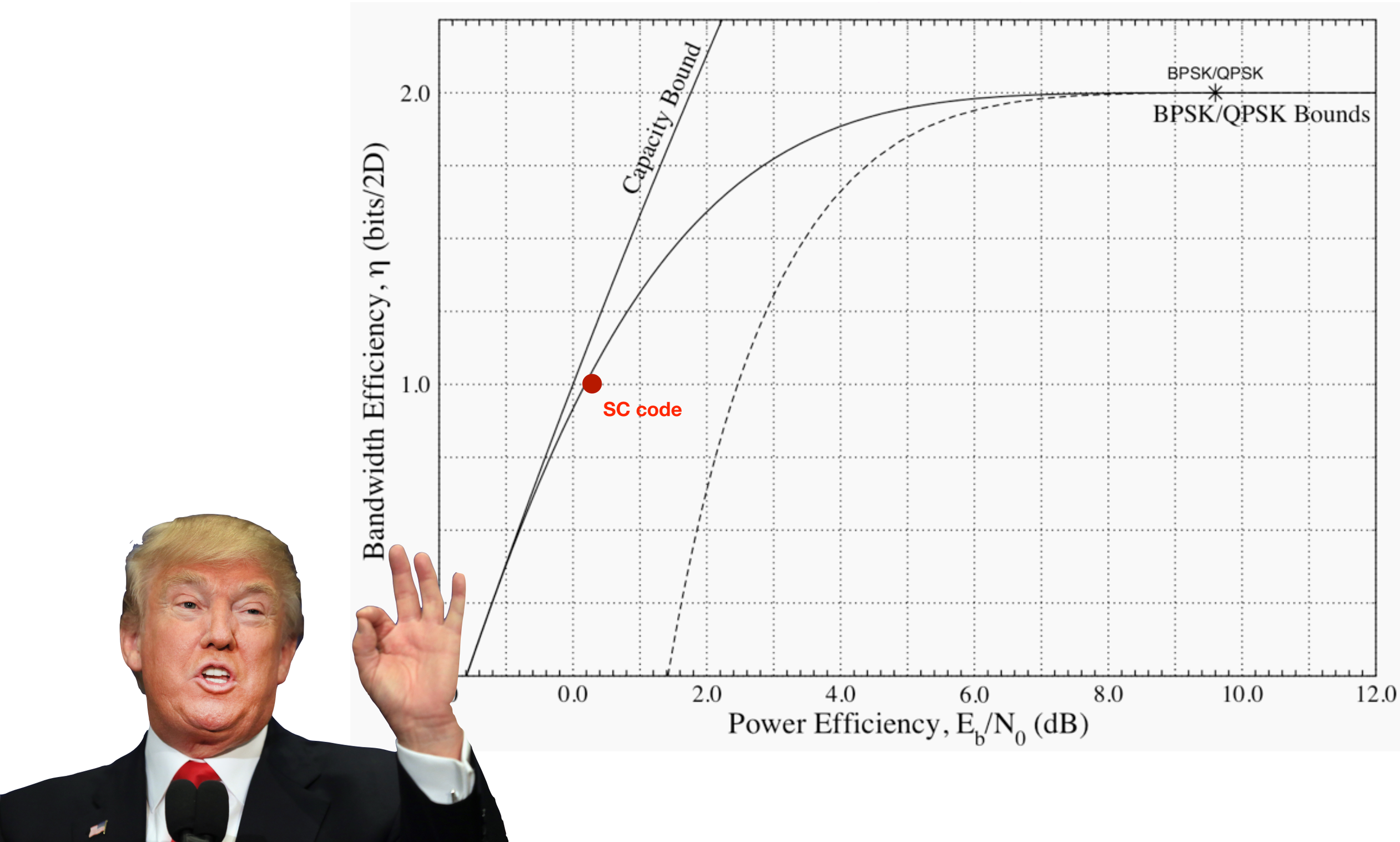
Political Views on Coding Theory

Donald Trump - *US Presidential Candidate (2016)*



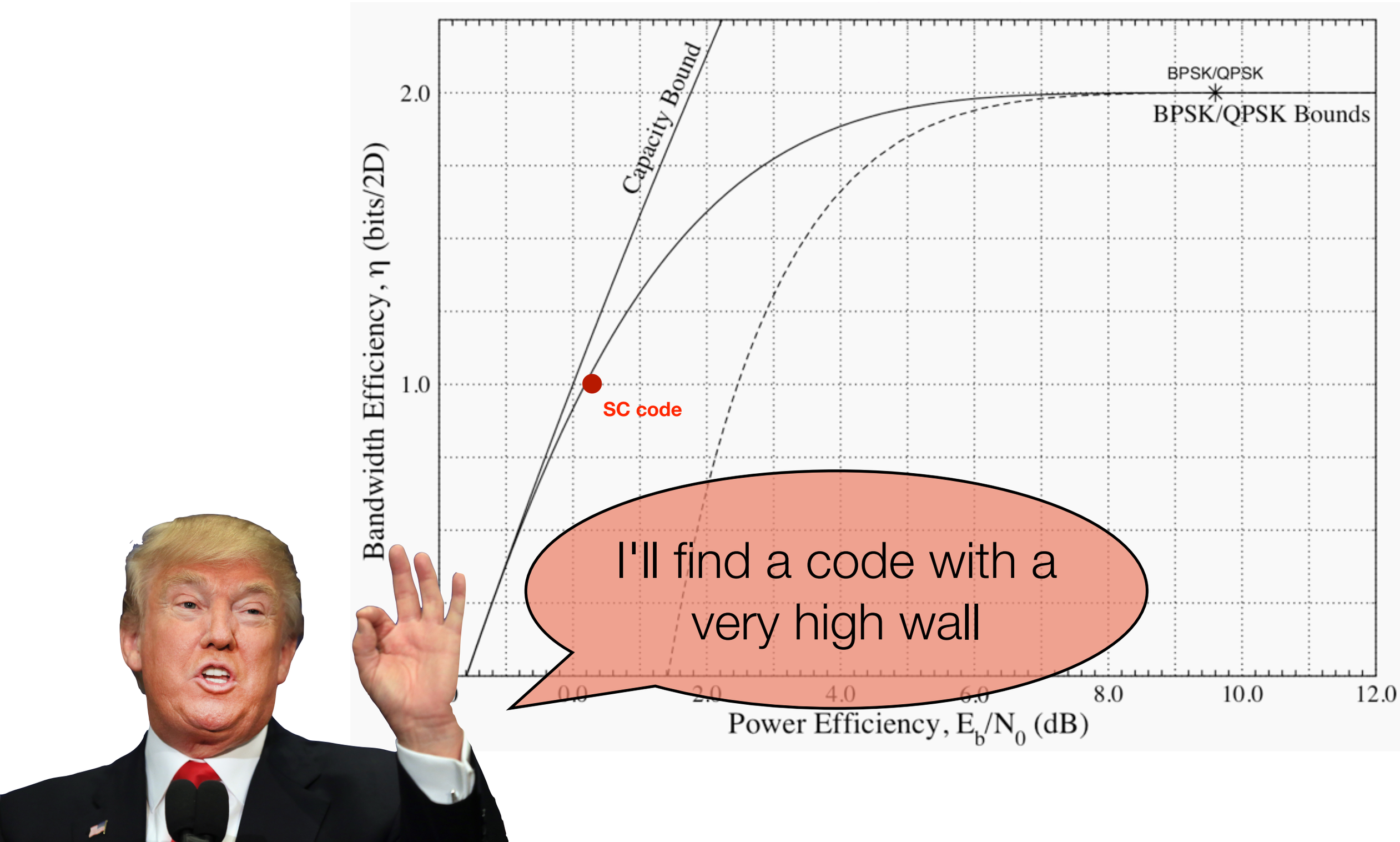
Political Views on Coding Theory

Donald Trump - *US Presidential Candidate (2016)*



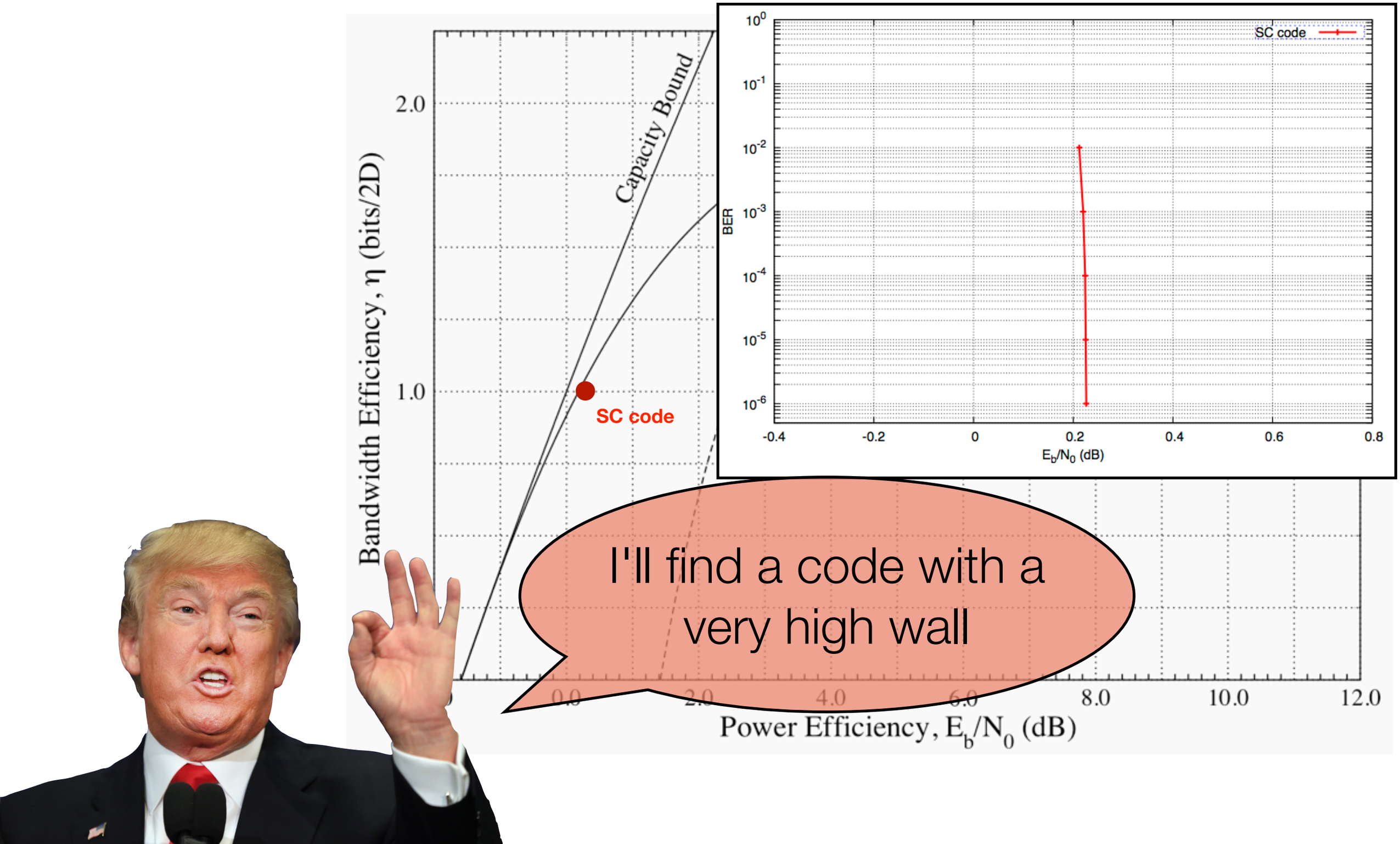
Political Views on Coding Theory

Donald Trump - *US Presidential Candidate (2016)*



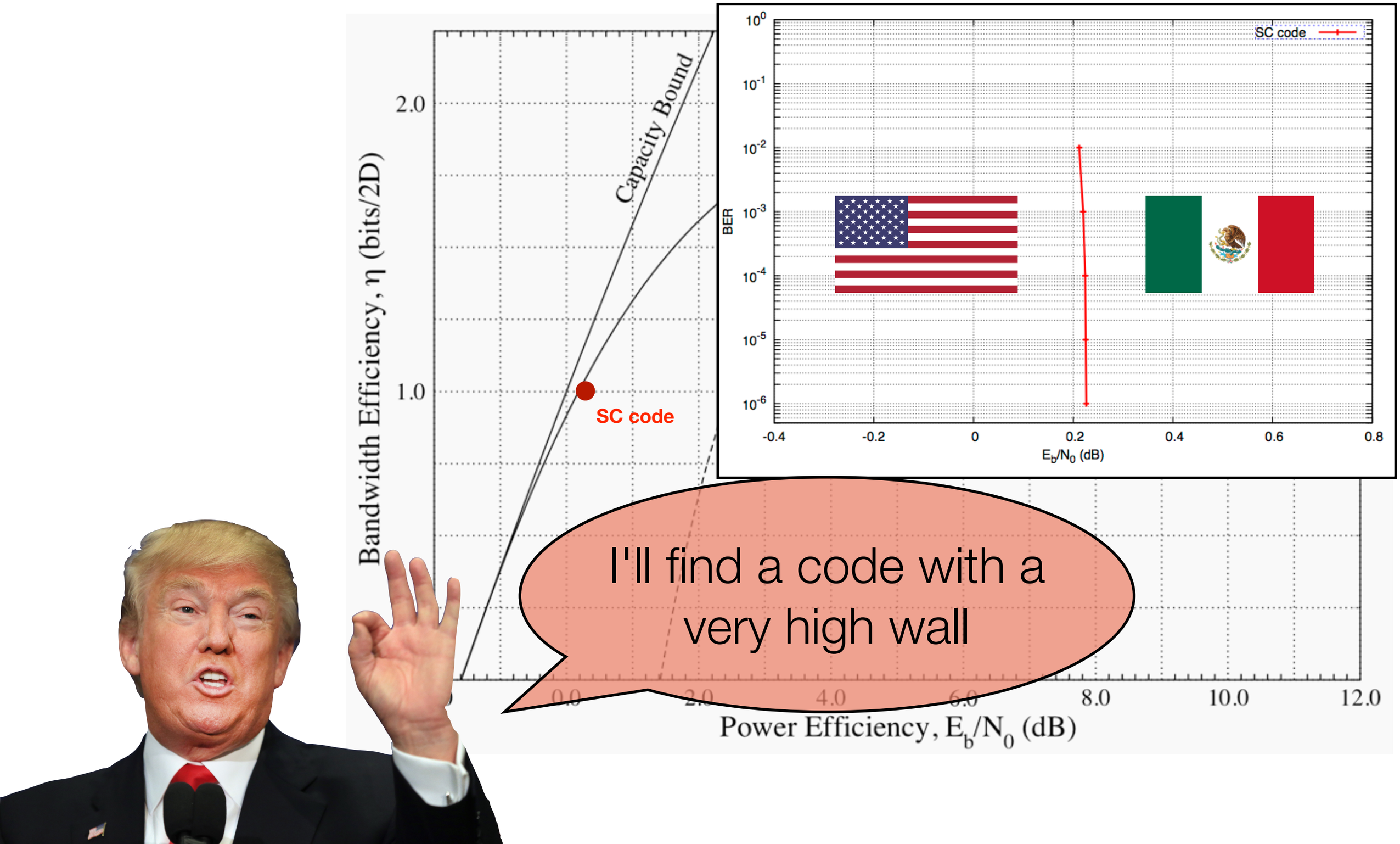
Political Views on Coding Theory

Donald Trump - *US Presidential Candidate (2016)*



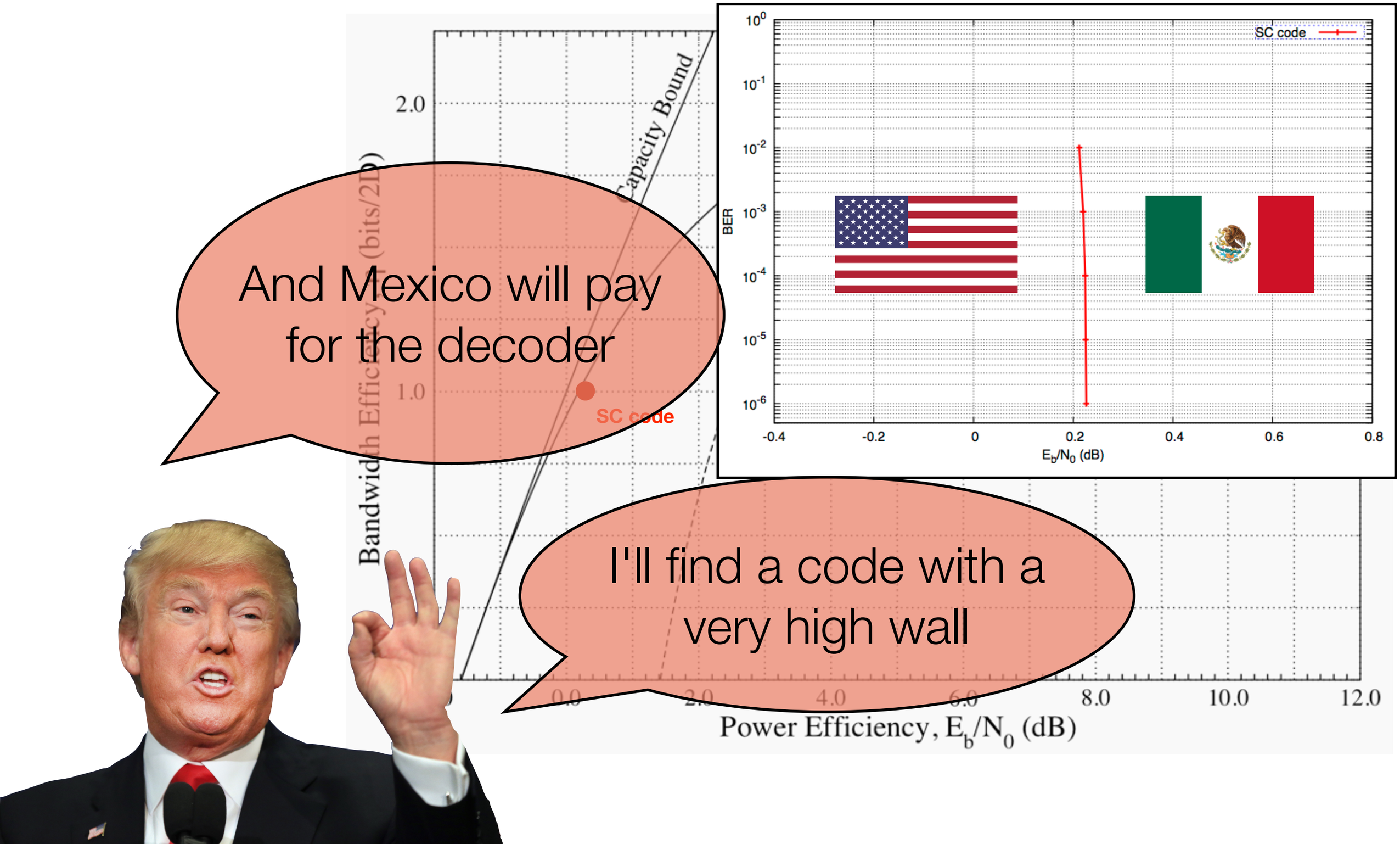
Political Views on Coding Theory

Donald Trump - *US Presidential Candidate (2016)*



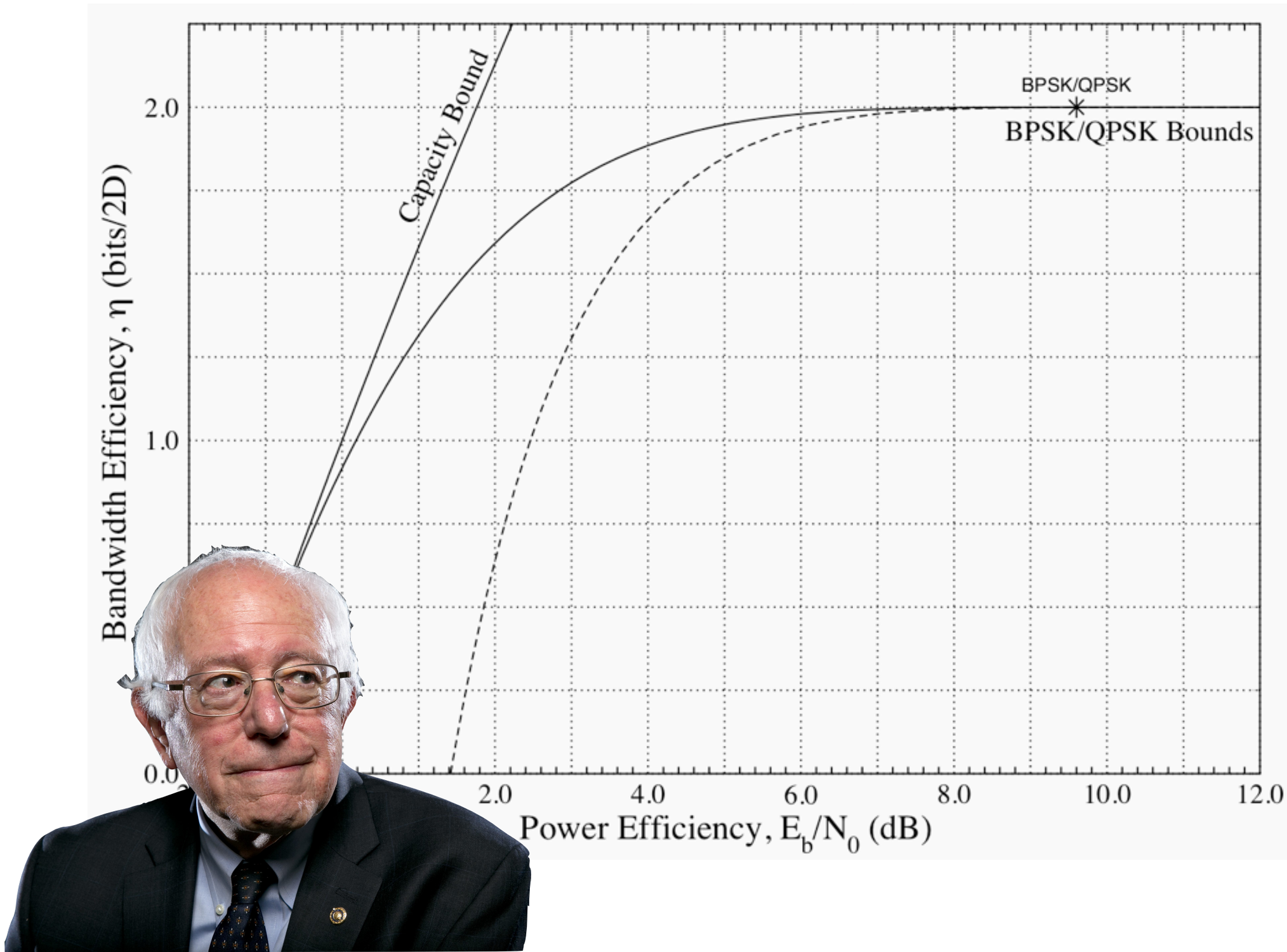
Political Views on Coding Theory

Donald Trump - *US Presidential Candidate (2016)*



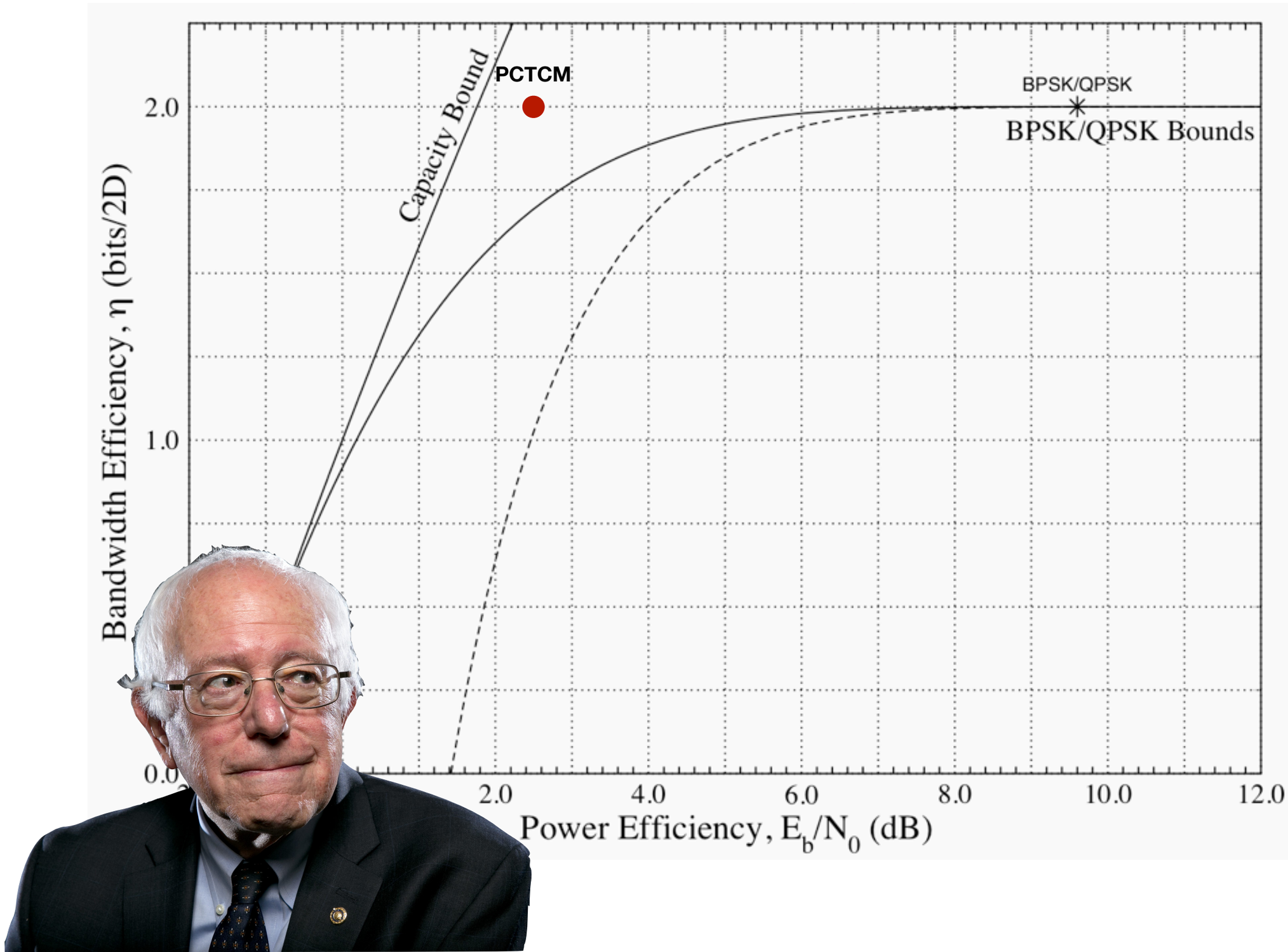
Political Views on Coding Theory

Bernie Sanders - *US Presidential Candidate (2016)*



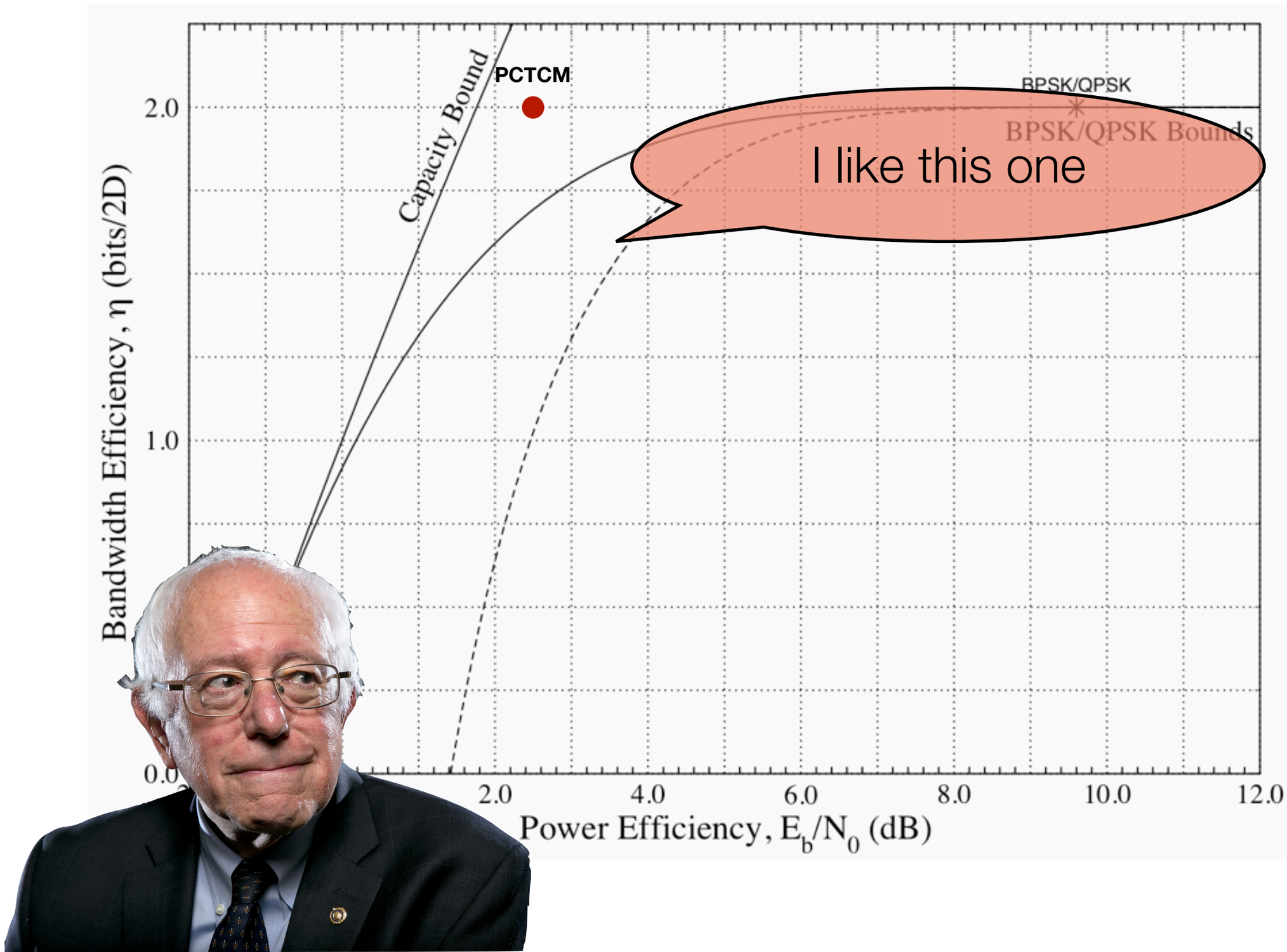
Political Views on Coding Theory

Bernie Sanders - *US Presidential Candidate (2016)*



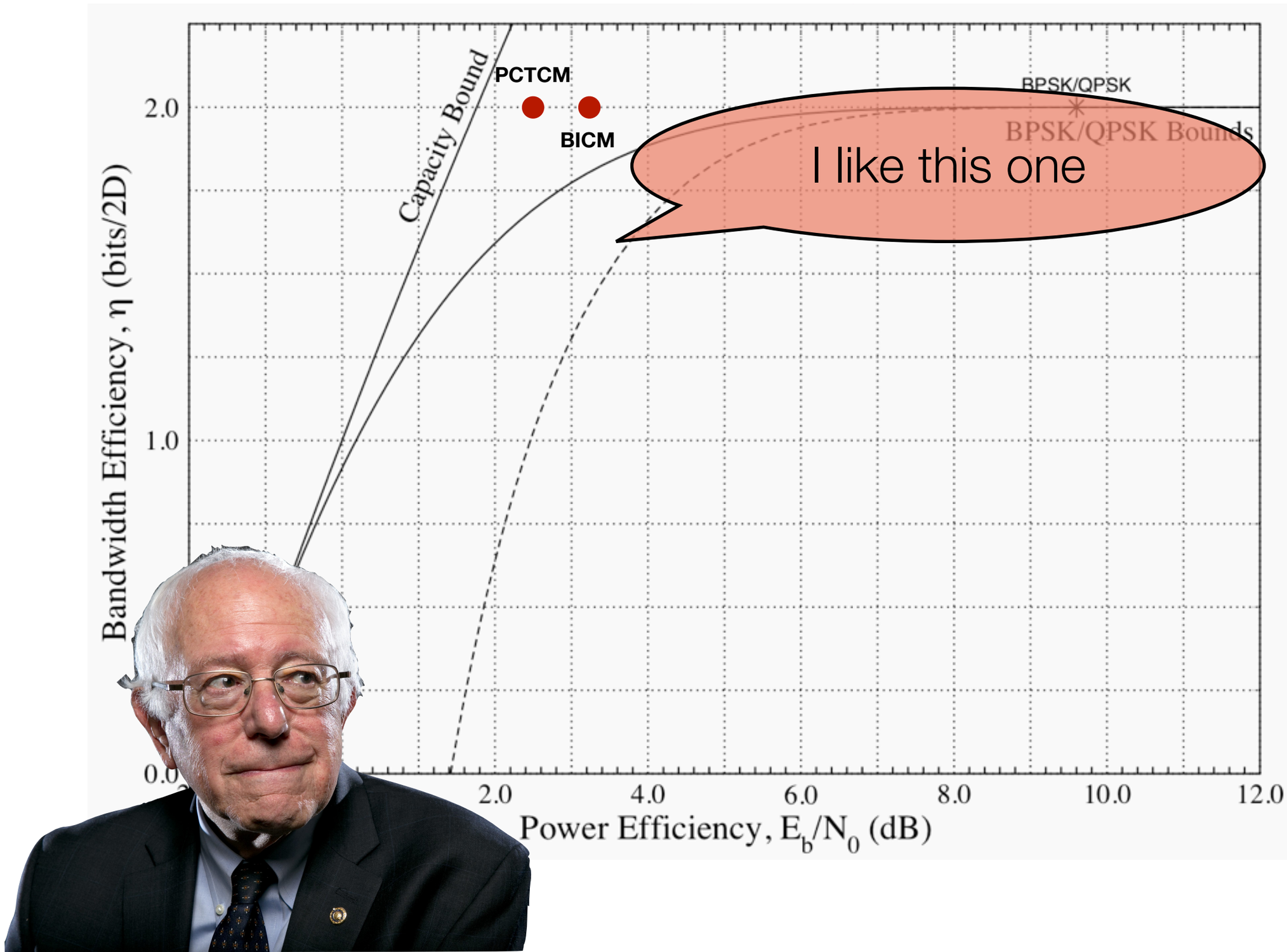
Political Views on Coding Theory

Bernie Sanders - *US Presidential Candidate (2016)*



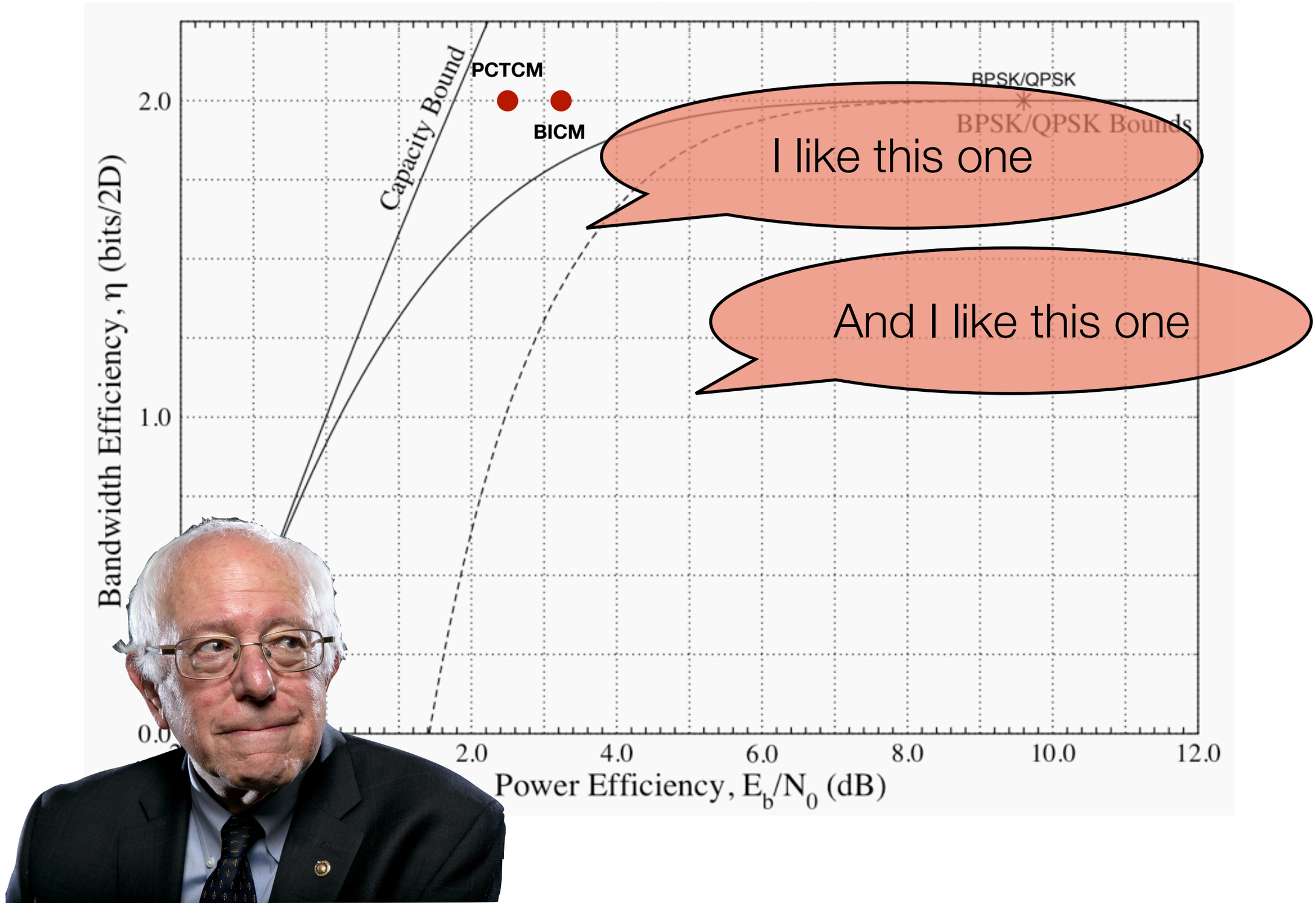
Political Views on Coding Theory

Bernie Sanders - *US Presidential Candidate (2016)*



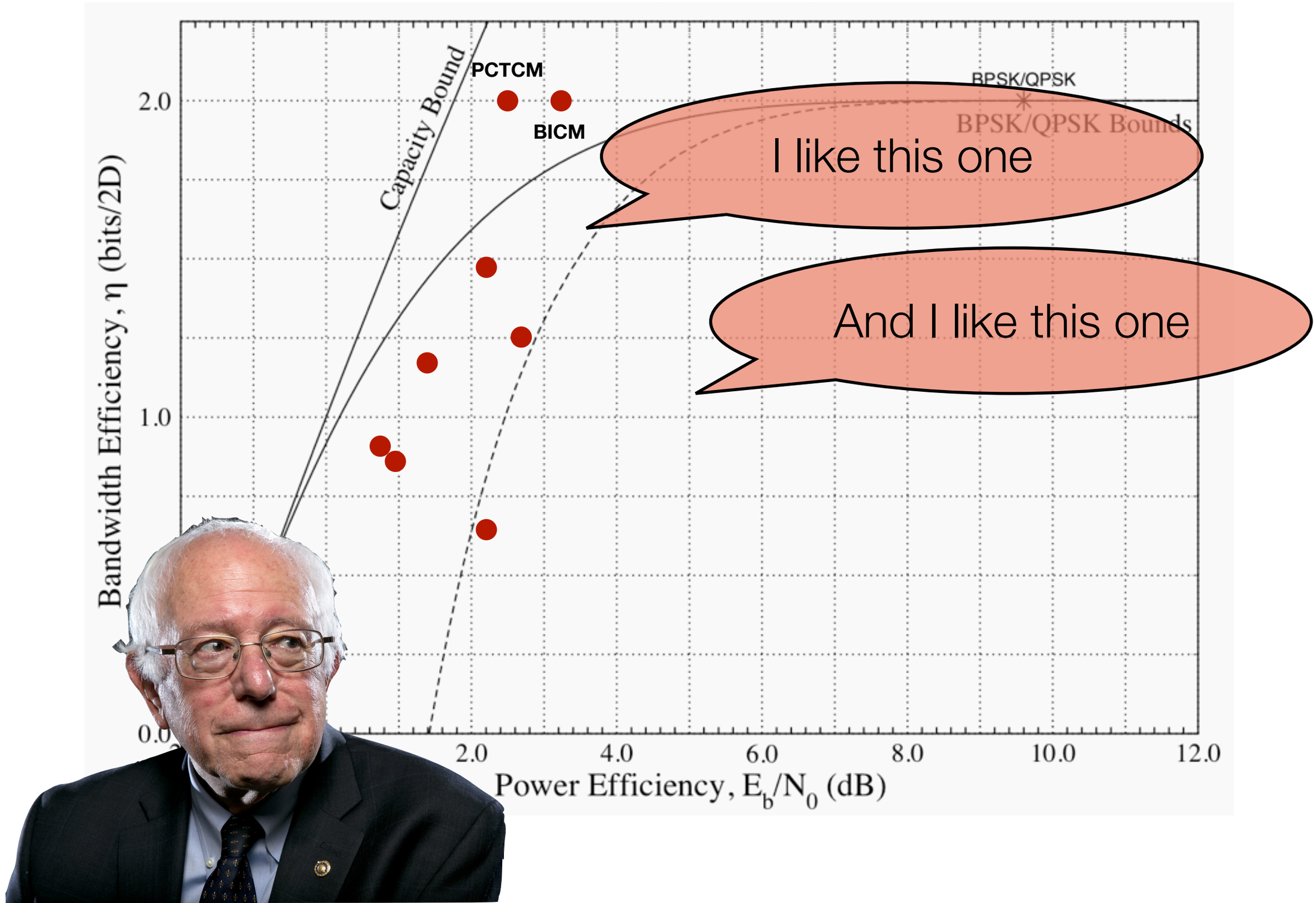
Political Views on Coding Theory

Bernie Sanders - *US Presidential Candidate (2016)*



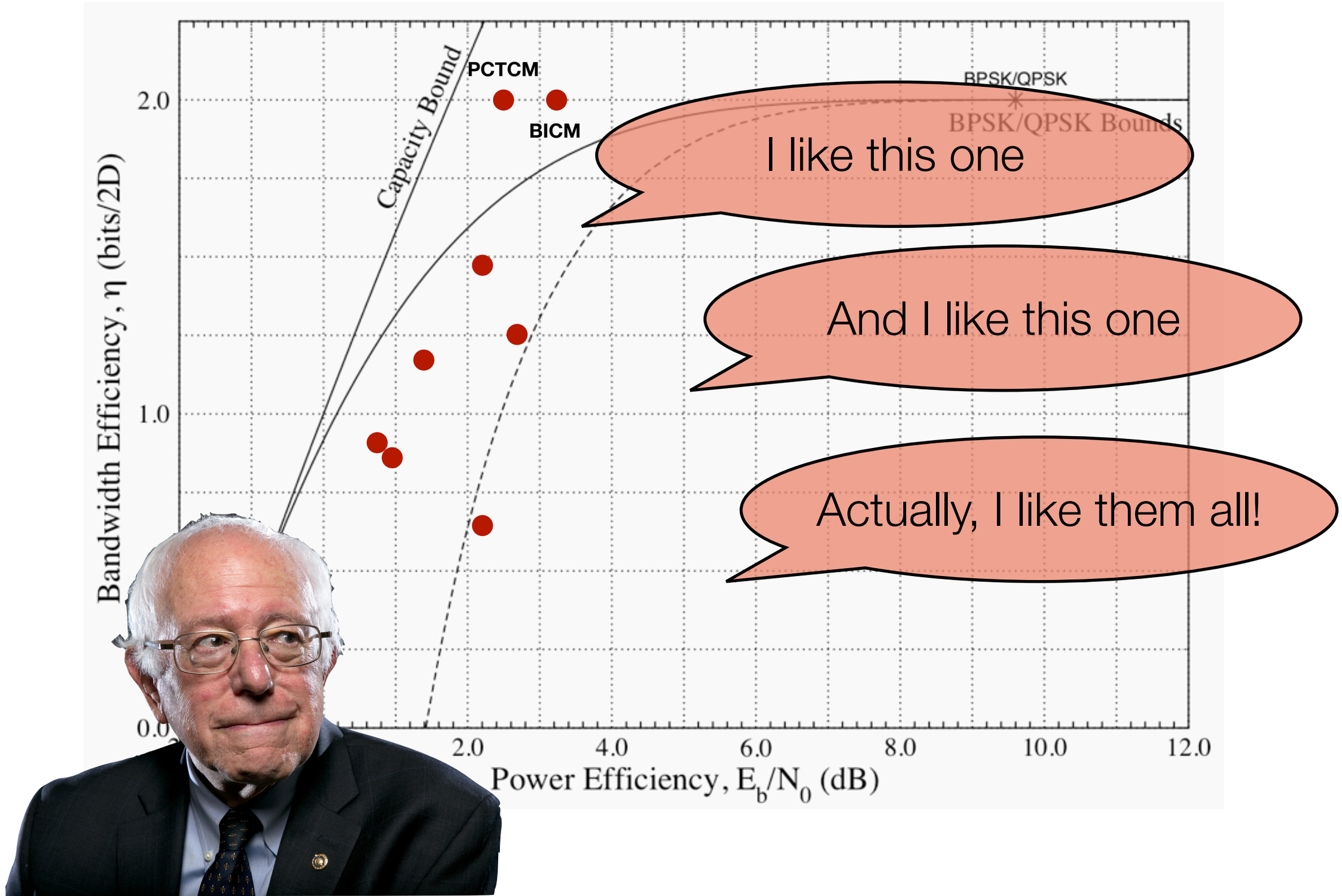
Political Views on Coding Theory

Bernie Sanders - *US Presidential Candidate (2016)*



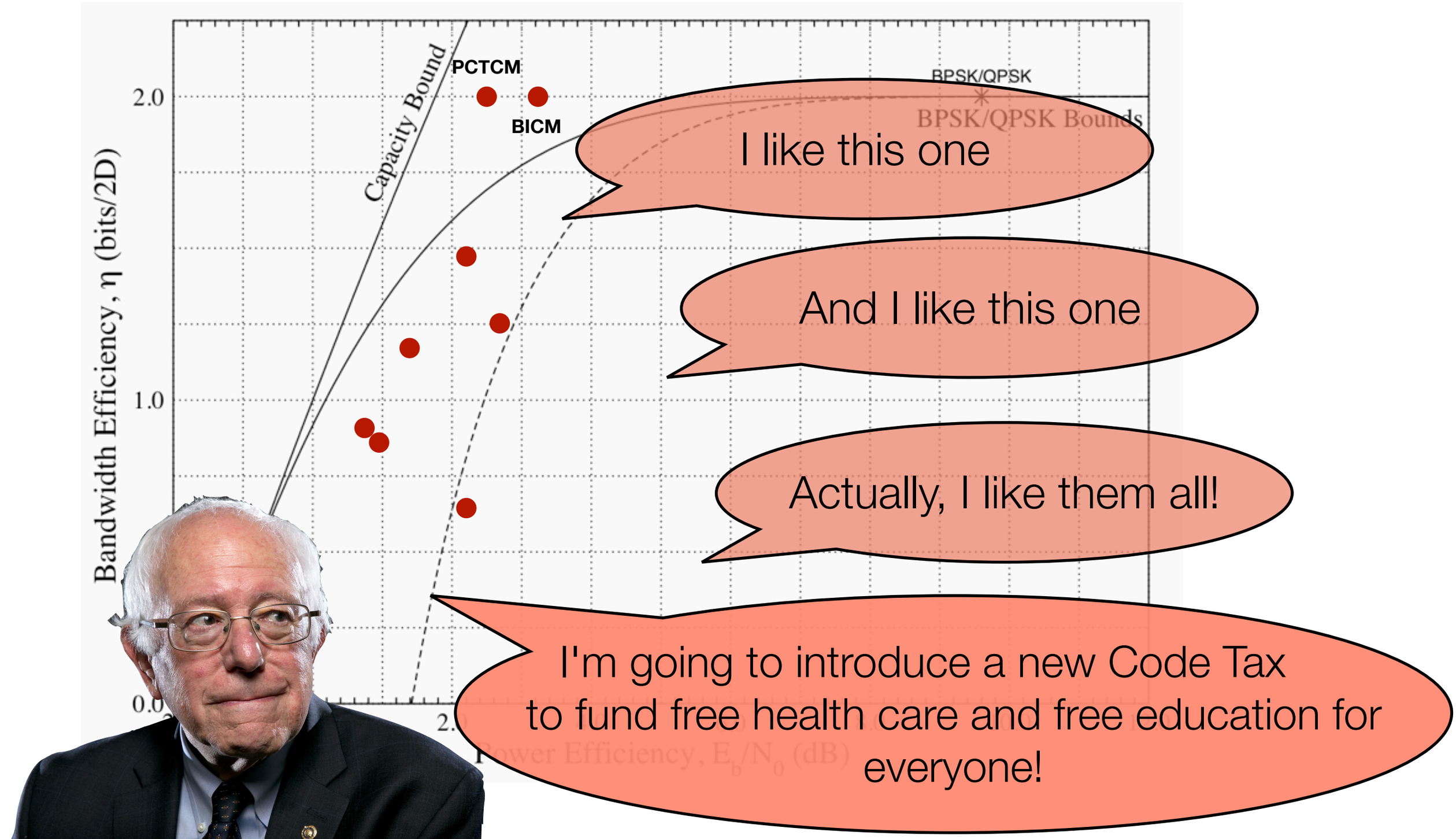
Political Views on Coding Theory

Bernie Sanders - *US Presidential Candidate (2016)*



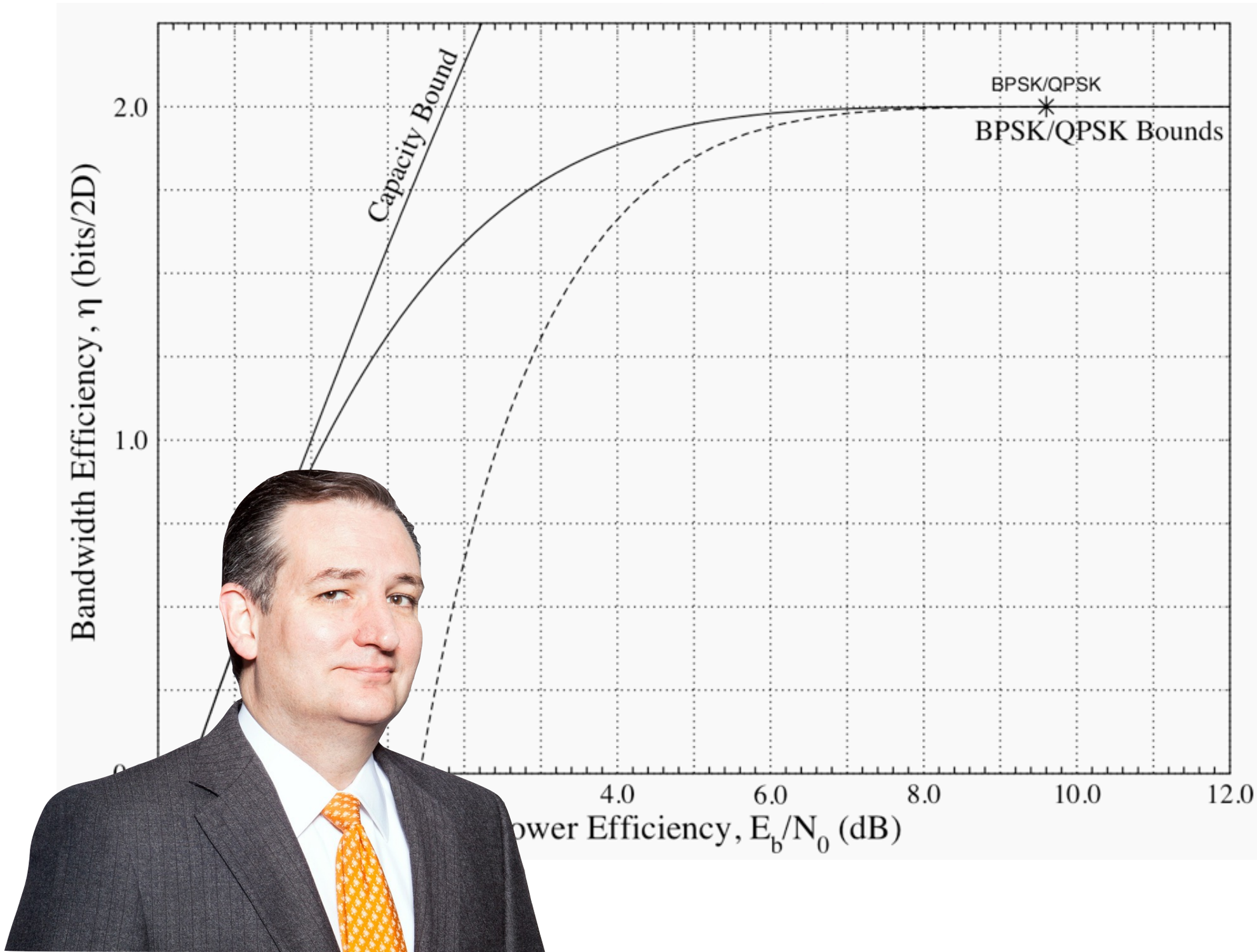
Political Views on Coding Theory

Bernie Sanders - *US Presidential Candidate (2016)*



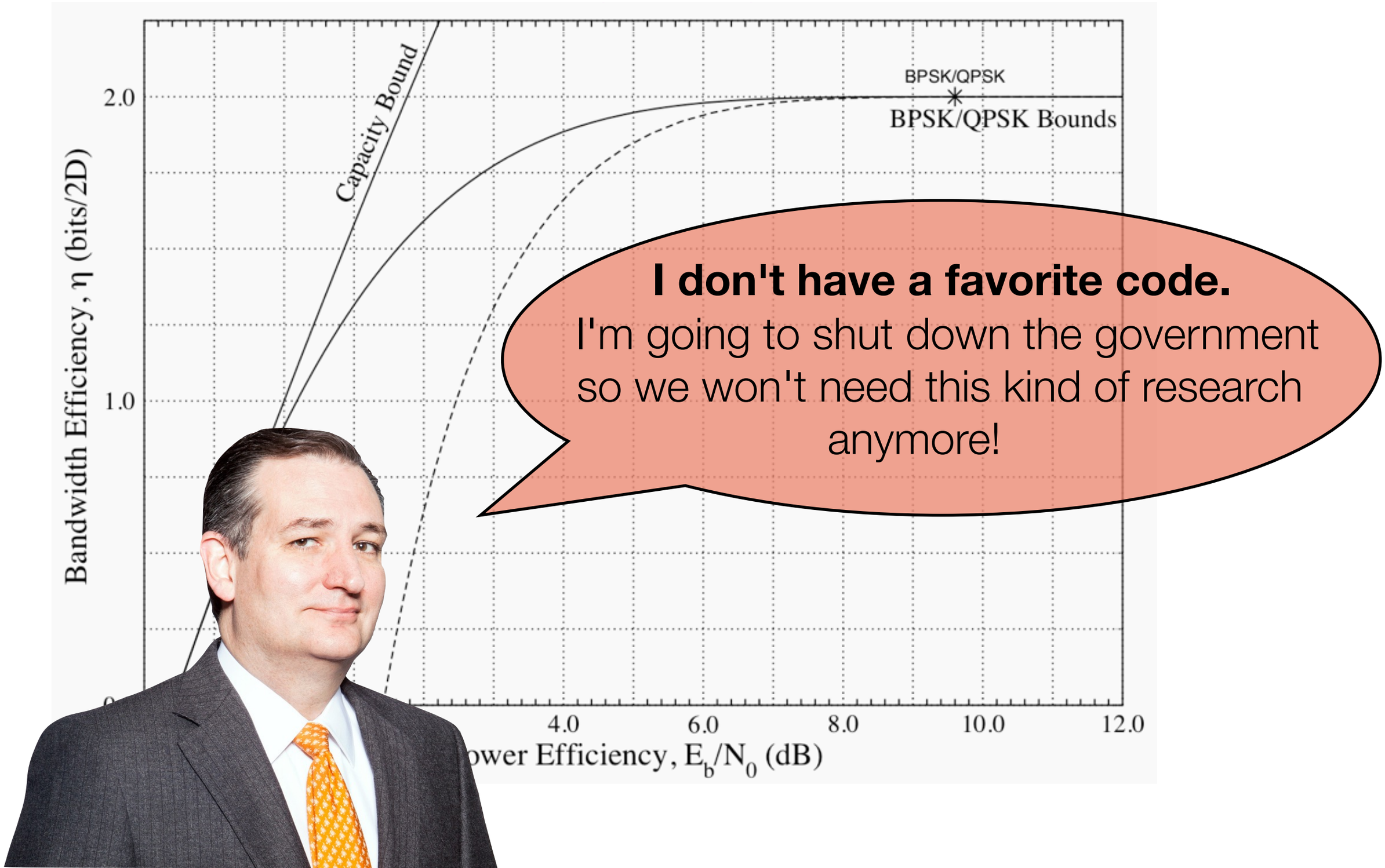
Political Views on Coding Theory

Ted Cruz - *US Presidential Candidate (2016)*



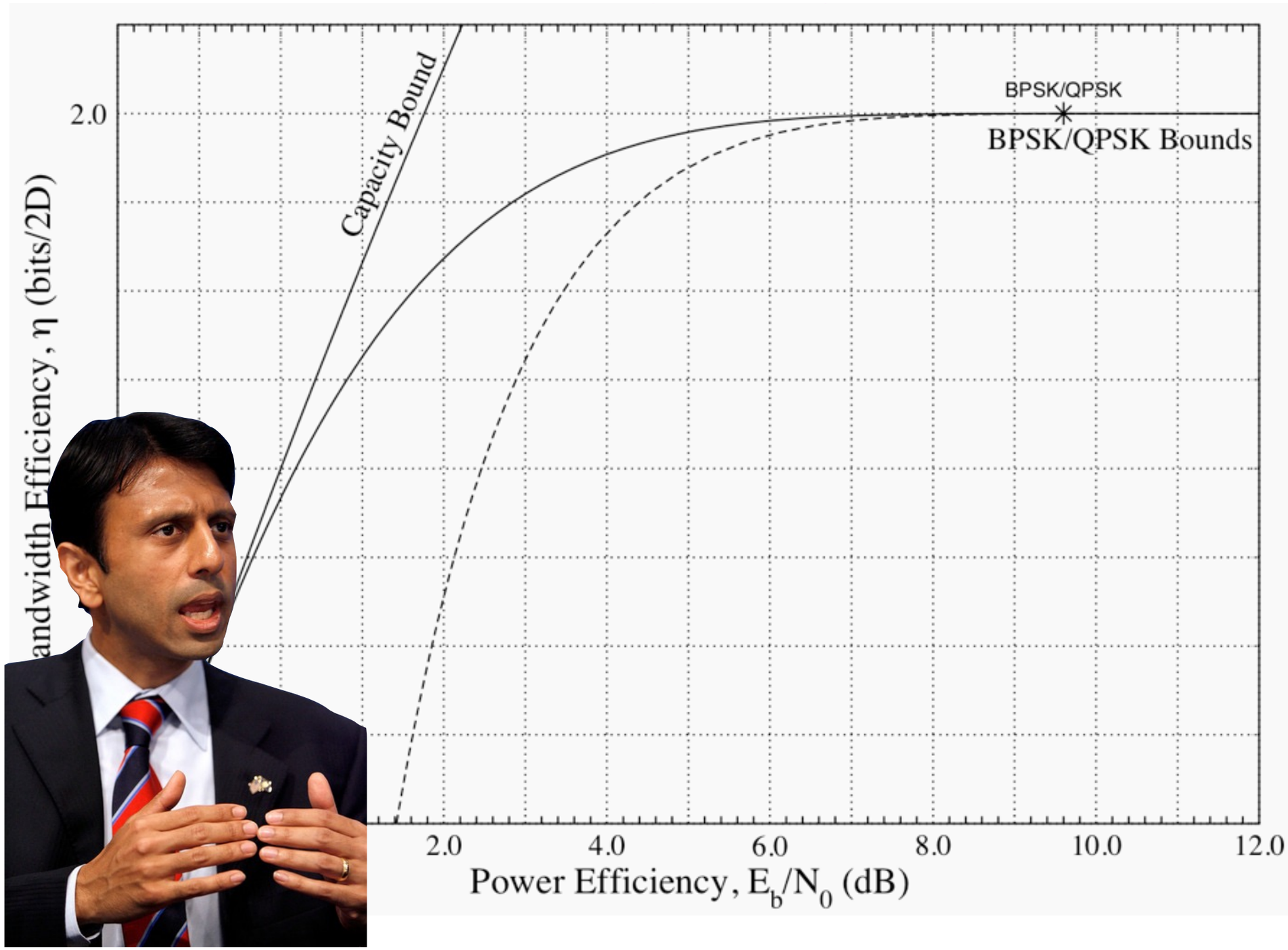
Political Views on Coding Theory

Ted Cruz - *US Presidential Candidate (2016)*



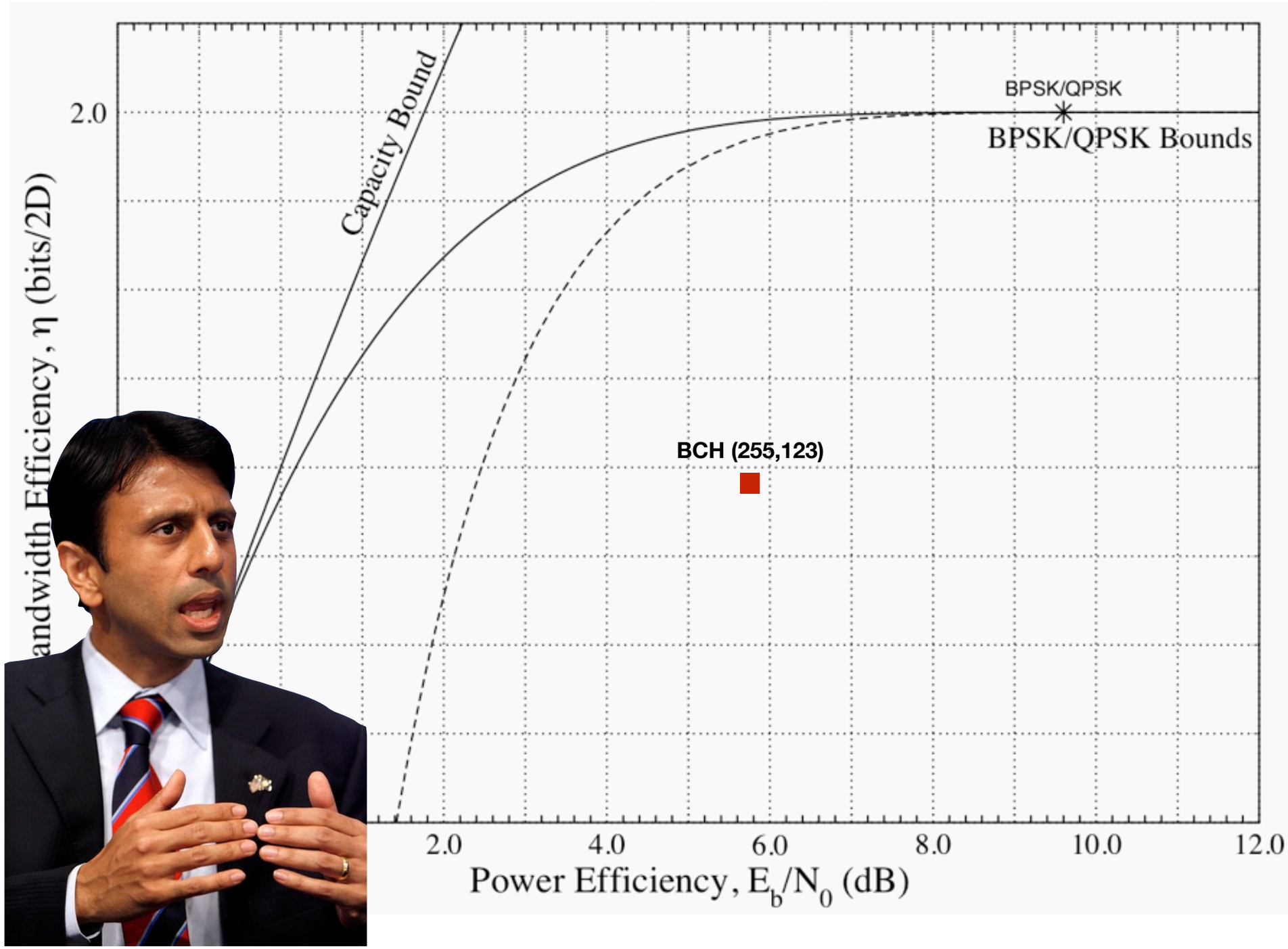
Political Views on Coding Theory

Bobby Jindal - *US Presidential Candidate (2016)*



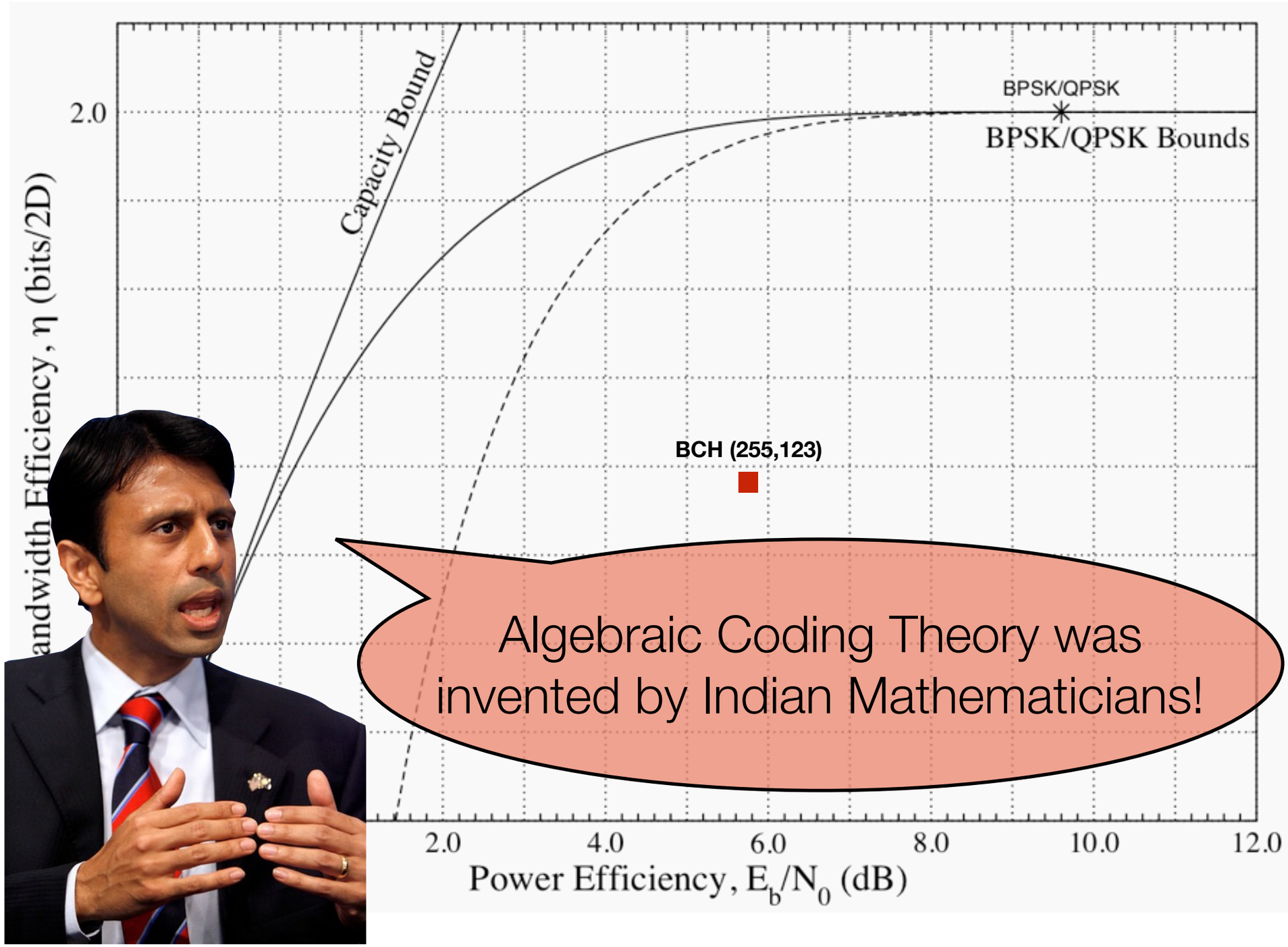
Political Views on Coding Theory

Bobby Jindal - *US Presidential Candidate (2016)*



Political Views on Coding Theory

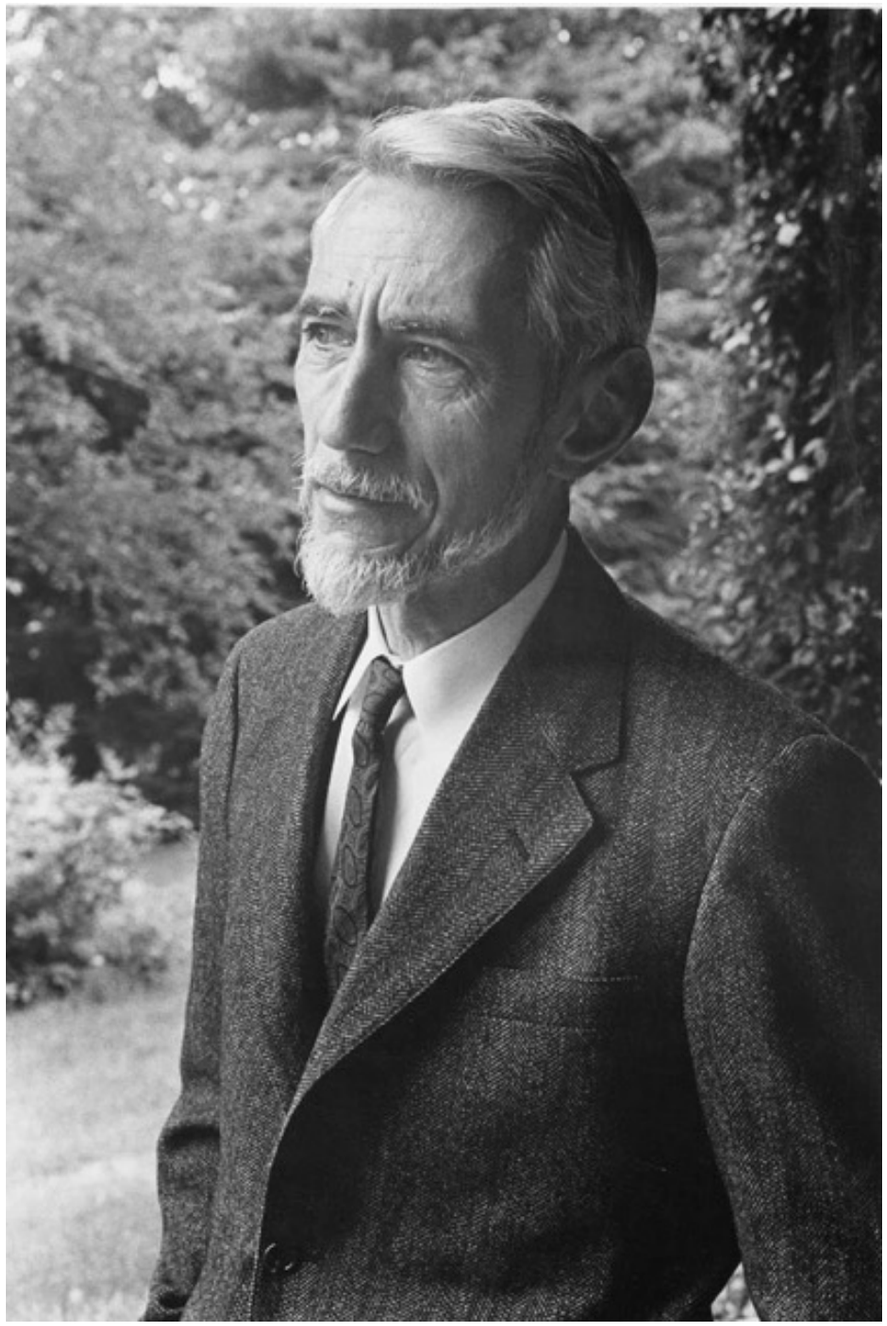
Bobby Jindal - *US Presidential Candidate (2016)*



Summary (The First Six Days)

- Algebraic Coding
- Convolutional (Shift Register) Codes
- Maximum Likelihood Decoding (Viterbi Alg.)
- Trellis Coded Modulation
- Soft Decision Decoding of Block Codes
- Turbo Codes and Iterative Decoding
- LDPC Codes and Codes on Graphs
- Polar Codes and Spatially Coupled Codes

The Seventh Day

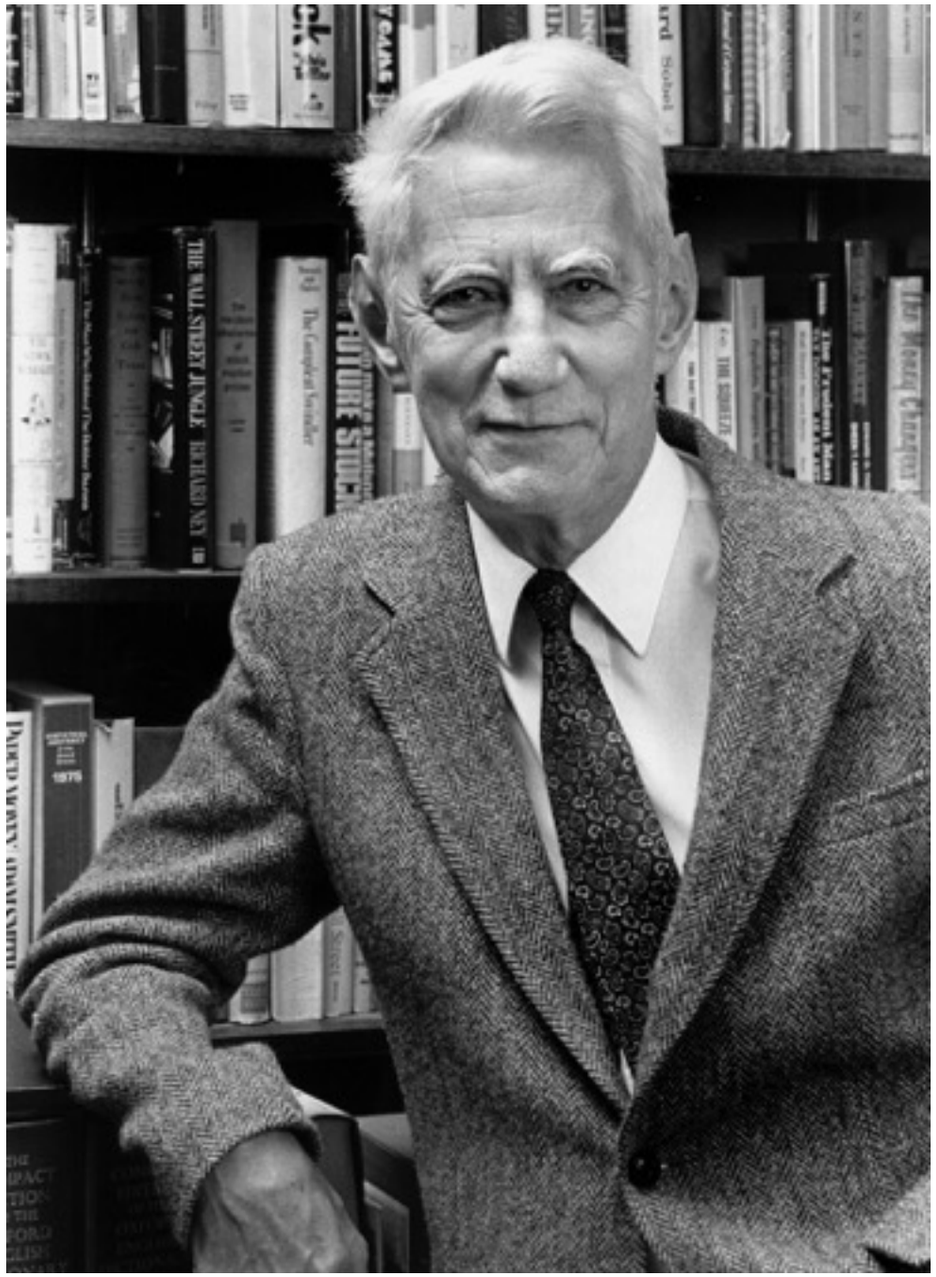


The Seventh Day

The Seventh Day

Rest...

The Eighth Day



The Eighth Day

Modern Code Designs

- Algebraic Geometry Codes
- Multi-Level Codes
- Turbo-Product Codes
- Generalized LDPC Codes
- Braided Codes
- Staircase Codes
- Fountain/Raptor (Rateless) Codes
- Space-Time Codes
- Polar Codes
- Spatially-Coupled Codes
- Locally-Decodable Codes

System Design Issues

- High Speed Decoding
- Linear Programming Decoding
- Parallel Decoder Architectures
- Analog Decoder Implementations
- Joint Source/Channel Coding
- Unequal Error Protection

Applications

- Satellite Communication
- Wireless Mobile Communication
- MIMO Channels
- Digital Video Broadcasting
- Digital Cable Transmission
- Network Coding
- Packet Erasure Channels
- Video Streaming
- Magnetic Recording
- Data Storage
- Flash Memories
- Fiber Optic Communication
- Quantum Coding
- Coding with a Delay Constraint
- Two-Dimensional Coding
- Power Line Communication