Quantum Computers and Cellular Phones

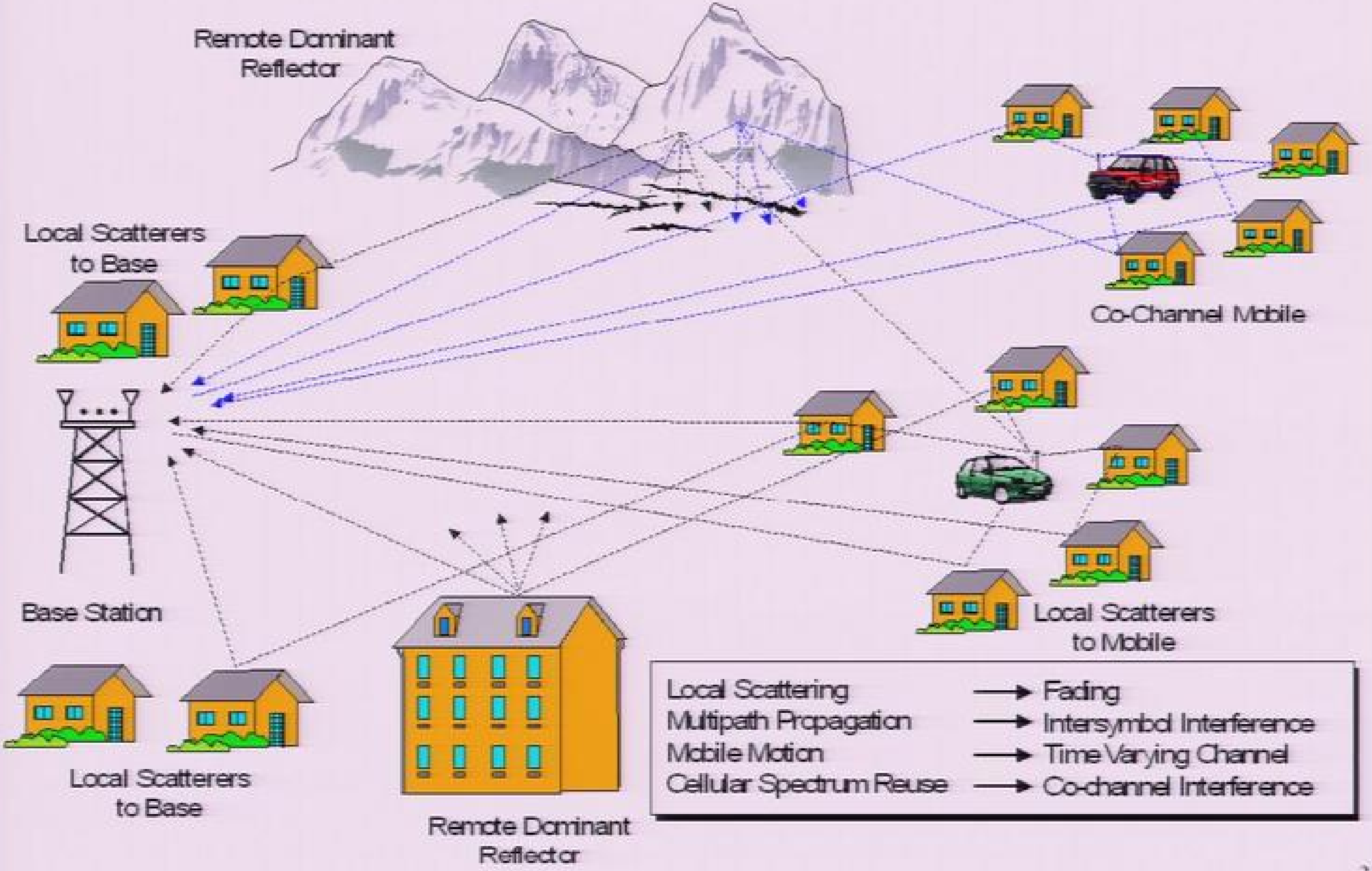
Robert Calderbank

Department of Electrical Engineering
Princeton University

Quantum Computers and Cellular Phones

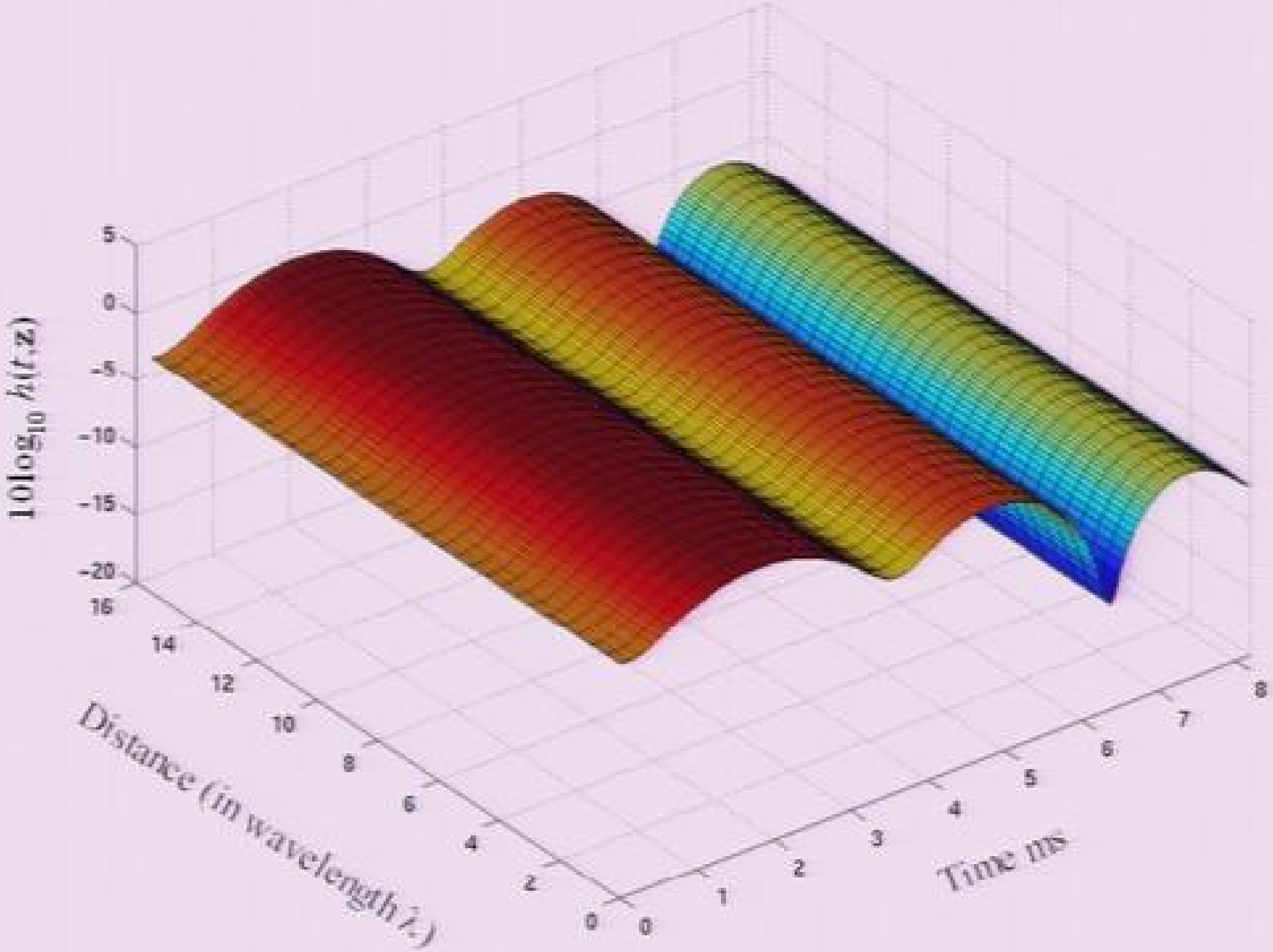
This talk explores the connection between quantum error correction and wireless systems that employ multiple antennas at the base station and the mobile terminal. The two topics have a common mathematical foundation, involving orthogonal geometry - the combinatorics of binary quadratic forms. We explain these connections, and describe how the wireless industry is making use of a mathematical framework developed by Radon and Hurwitz about a hundred years ago.

Wireless Channels



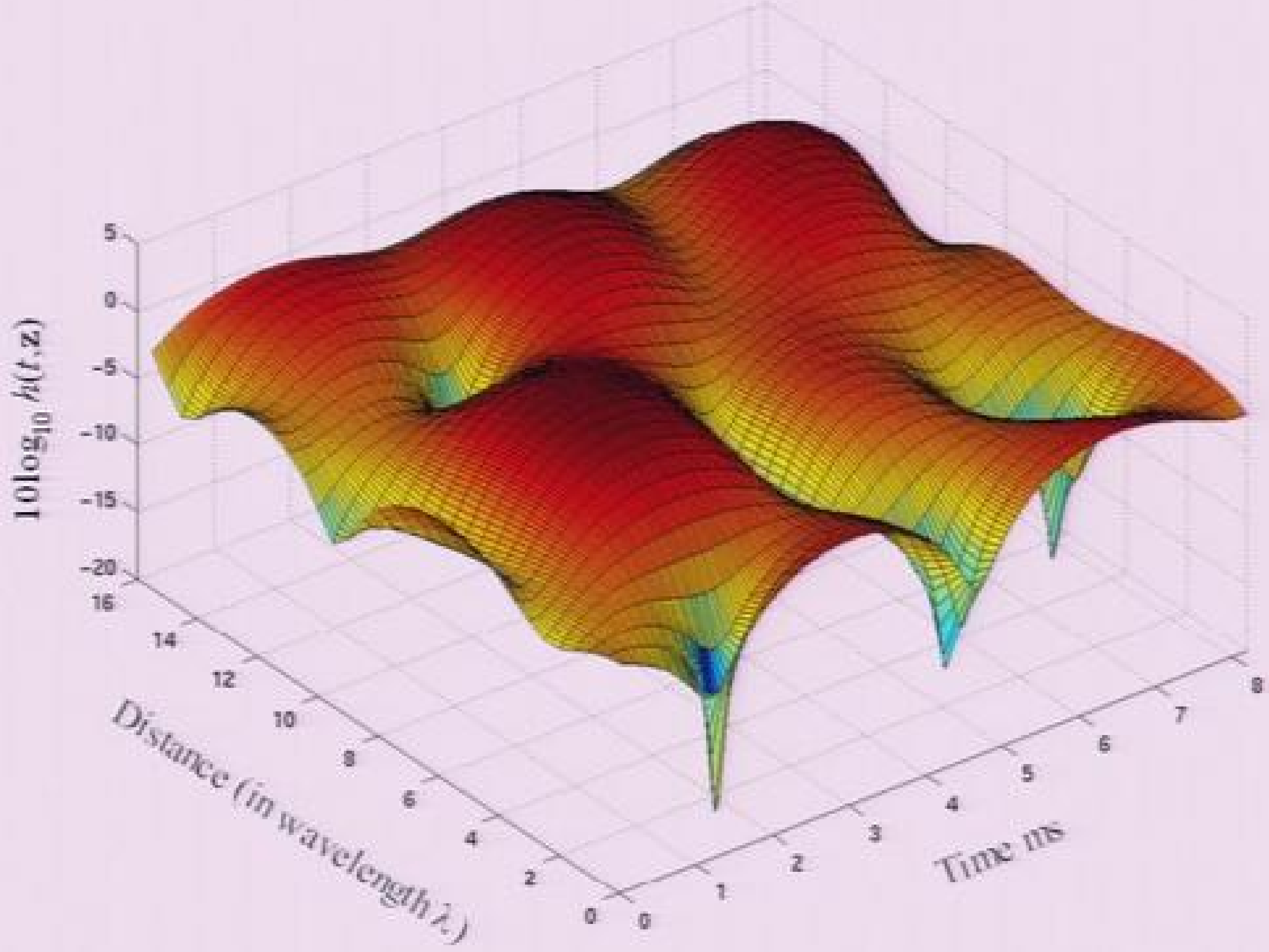
Local Scattering → Fading
Multipath Propagation → Intersymbol Interference
Mobile Motion → Time Varying Channel
Cellular Spectrum Reuse → Co-channel Interference

Space-Time Fading



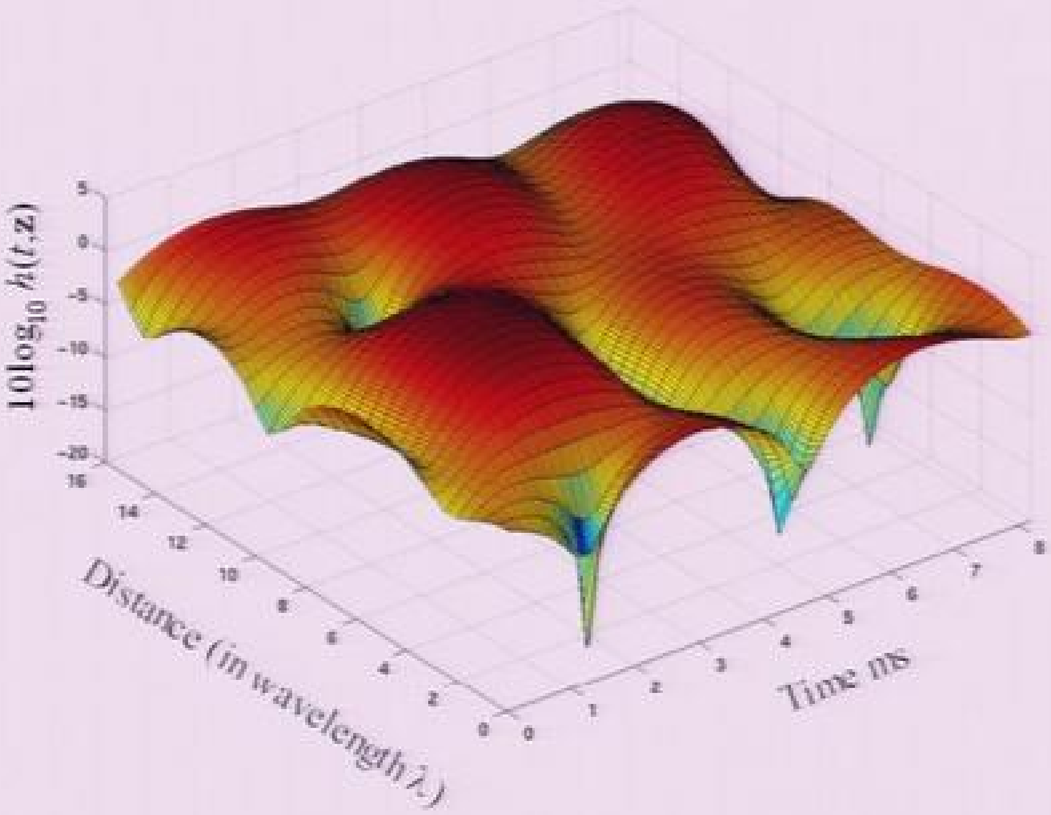
Angle Spread $\Theta_d = 0°$, Doppler Spread $f_d = 200$ Hz

Space-Time Fading



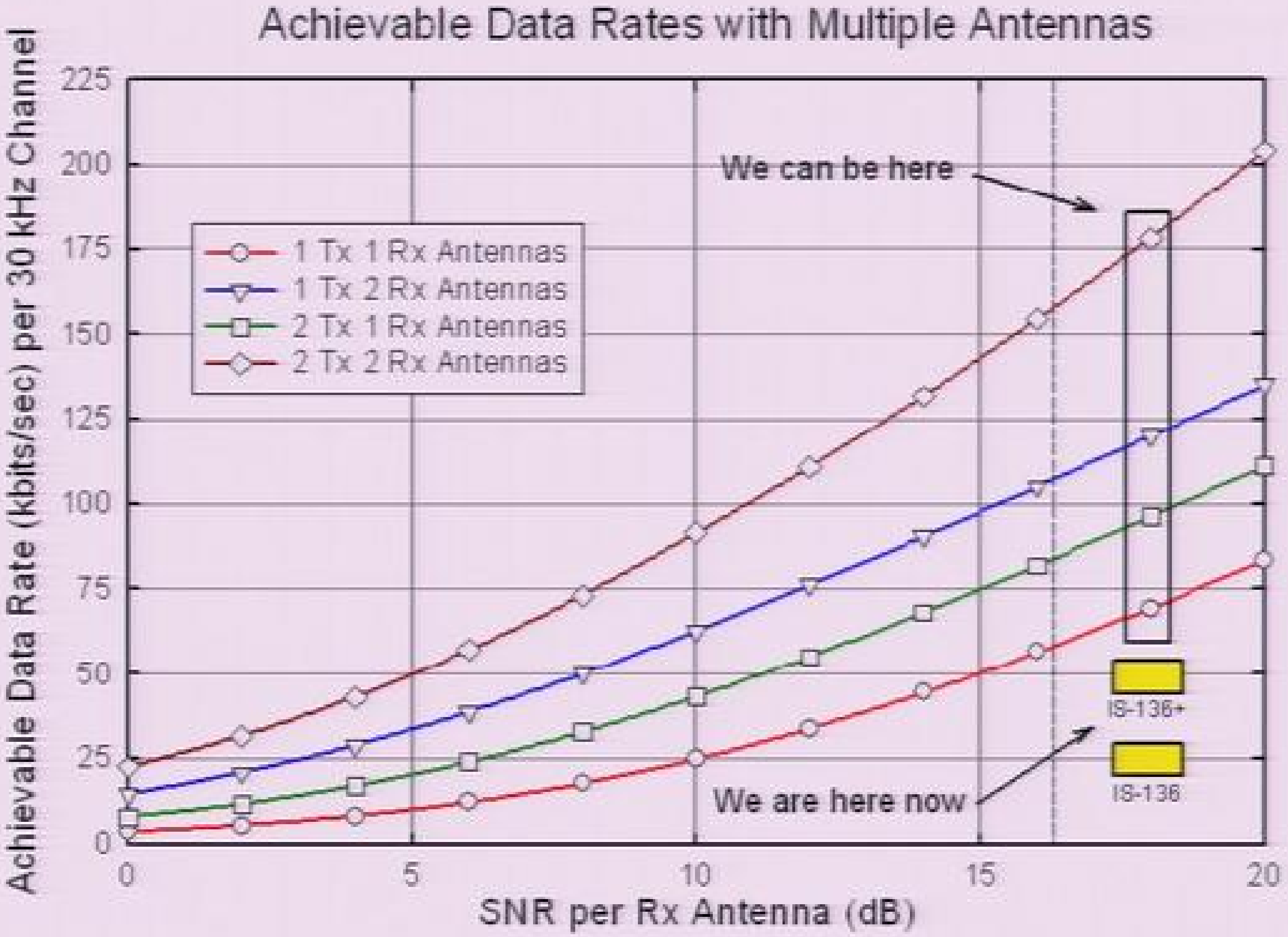
Angle Spread Θ_d = 5°, Doppler Spread f_d = 200 Hz

What is Space-Time Coding?



- **Correlate symbols across time and space**. Use the symbols when the channel is good to recover the symbols when the channel is bad.

Fundamental Limits: Outage Capacity



"It is dangerous to put limits on wireless"

Guglielmo Marconi (1932)

STC: The Model …

- Transmitted Code Vector:

$$\mathbf{c}_l = [\ c_1(l), c_2(l), \cdots\ , c_N(l)\,]^T$$

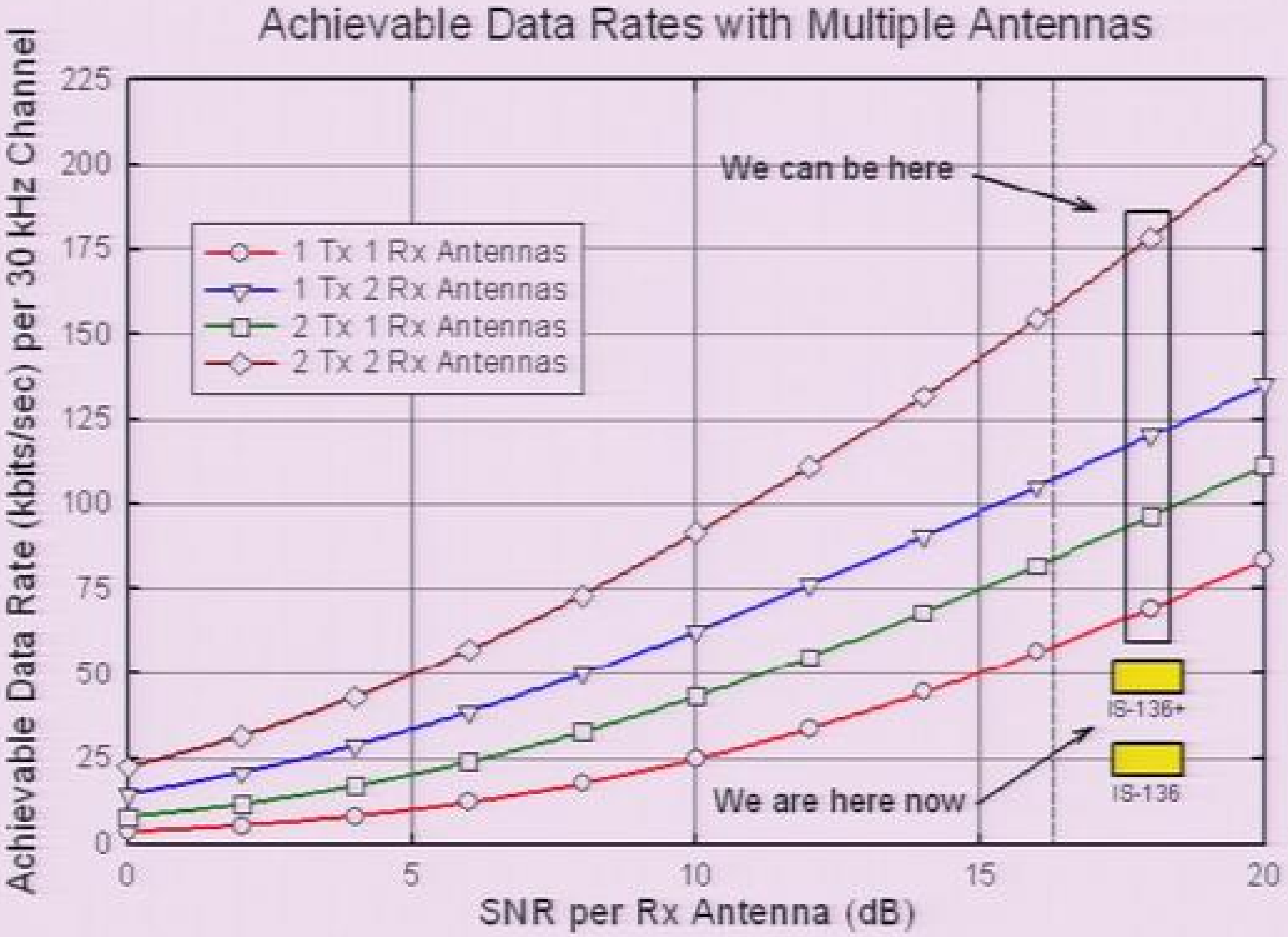
- Channel Matrix:

$$\mathbf{H} = \begin{array}{cc} \text{transmit} & \\ \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1N} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{M1} & \alpha_{M2} & \cdots & \alpha_{MN} \end{pmatrix} & \text{receive} \end{array}$$

- Received Signal Vector:

$$\mathbf{r}(l) = \mathbf{H} \cdot \mathbf{c}_l + \mathbf{n}(l)$$

Fundamental Limits: Outage Capacity



“It is dangerous to put limits on wireless”

Guglielmo Marconi (1932)

STC: The Model …

- Transmitted Code Vector:

$$\mathbf{c}_l = [\, c_1(l),\, c_2(l),\, \cdots\, ,\, c_N(l)\,]^T$$

- Channel Matrix:

$$\mathbf{H} = \begin{array}{cc} \downarrow\text{transmit} & \\ \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1N} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{M1} & \alpha_{M2} & \cdots & \alpha_{MN} \end{pmatrix} & \text{receive} \end{array}$$

- Received Signal Vector:

$$\mathbf{r}(l) = \mathbf{H} \cdot \mathbf{c}_l + \mathbf{n}(l)$$

STC: Probability of Error Analysis ….

- The matrix **B** is the error matrix between the transmitted code vector sequence **C** and the decoded code vector sequence $\widetilde{\mathbf{C}}$.

$$\mathbf{B} = \begin{bmatrix} c_1(1)-\widetilde{c}_1(1) & c_1(2)-\widetilde{c}_1(2) & \cdots & c_1(L)-\widetilde{c}_1(L) \\ c_2(1)-\widetilde{c}_2(1) & c_2(2)-\widetilde{c}_2(2) & \cdots & c_2(L)-\widetilde{c}_2(L) \\ \vdots & \vdots & \ddots & \vdots \\ c_N(1)-\widetilde{c}_N(1) & c_N(2)-\widetilde{c}_N(2) & \cdots & c_N(L)-\widetilde{c}_N(L) \end{bmatrix}$$

STC: Probability of Error Analysis

- Transmitted code vector sequence: $\mathbf{C} = \{\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_L\}$.
- Probability of error: assuming perfect knowledge of CSI.

$$\Pr\ (\mathbf{C}\to \tilde{\mathbf{C}}|\mathbf{H}) \le \exp[-d^2(\mathbf{C},\tilde{\mathbf{C}})]$$

$$d^2(\mathbf{C},\tilde{\mathbf{C}}) = \sum_{j=1}^{M}\sum_{l=1}^{L}\left|\alpha_{j1}[c_1(l)-\tilde{c}_1(l)] + \cdots\cdots + \alpha_{jN}[c_N(l)-\tilde{c}_N(l)]\right|^2$$

$$= \sum_{j=1}^{M}\mathbf{h}_j\,\mathbf{A}(\mathbf{C},\tilde{\mathbf{C}})\,\mathbf{h}_j^*, \quad \text{where}$$

$$\mathbf{h}_j = [\ \alpha_{j1}\ \alpha_{j2}\ \cdots\ \alpha_{jN}\ ]^T$$

$$\mathbf{A}(\mathbf{C},\tilde{\mathbf{C}}) = \mathbf{B}(\mathbf{C},\tilde{\mathbf{C}})\mathbf{B}^*(\mathbf{C},\tilde{\mathbf{C}})$$

STC: Probability of Error Analysis ....

- Probability of error:

$$\Pr(\mathbf{C} \to \widetilde{\mathbf{C}}) \leq \left(\prod_{i=1}^{N} \frac{1}{1 + \lambda_i \cdot \Gamma_s}\right)^{M}$$

- Let r be the rank of the matrix **A** and $\lambda_1, \lambda_2, \ldots, \lambda_r$ be the nonzero eigenvalues of **A**. Then

$$\Pr(\mathbf{C} \to \widetilde{\mathbf{C}}) \leq \left(\prod_{i=1}^{r} \lambda_i\right)^{-M} \cdot \Gamma_s^{-rM}$$

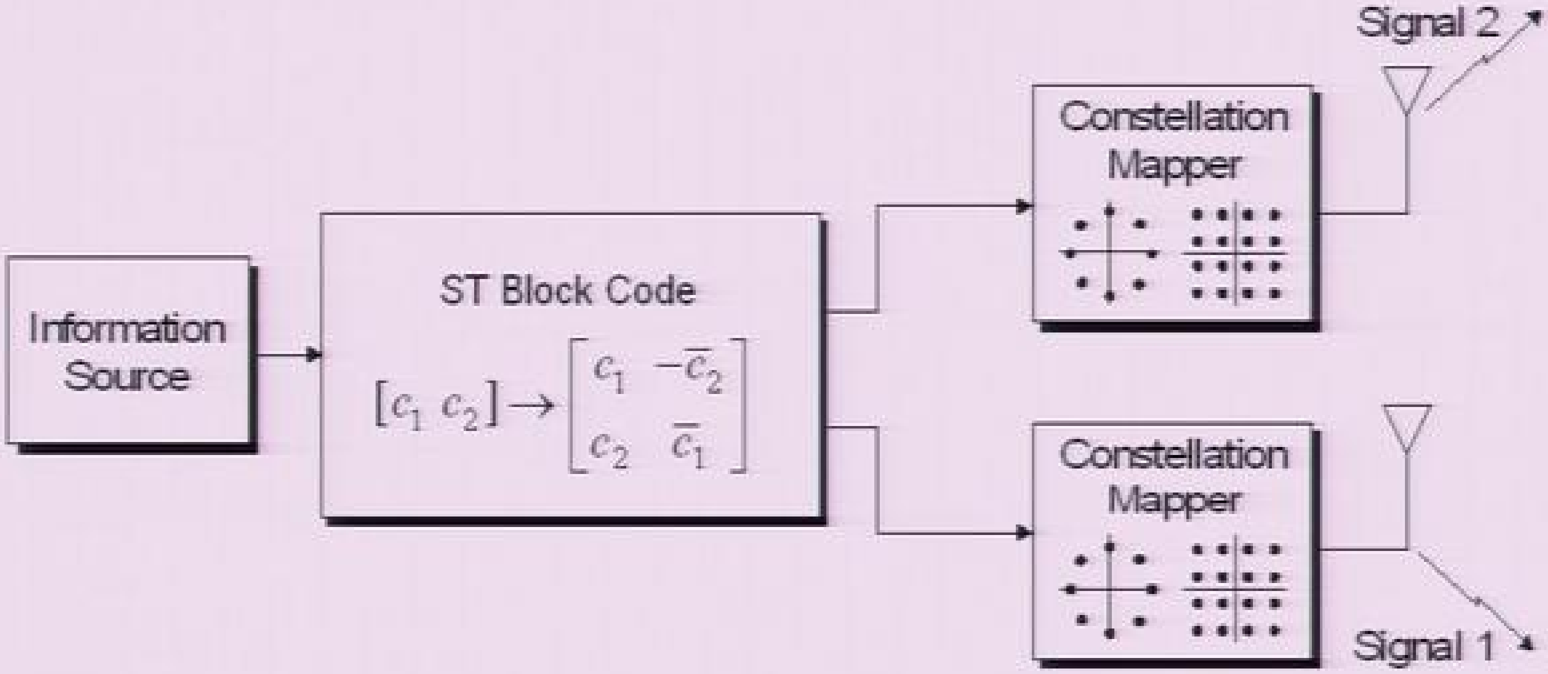
- Thus a diversity gain of rM and a coding gain of $(\lambda_1 \lambda_2 \ldots \lambda_r)^{1/r}$ are achieved.

STC: Design Criteria

;

- Rank Criterion: In order to achieve the maximum diversity NM, the matrix $\mathbf{B}(\mathbf{C}_1,\mathbf{C}_2)$ has to be full rank for any two code vector sequences $\mathbf{C}_1$ and $\mathbf{C}_2$. If $\mathbf{B}(\mathbf{C}_1,\mathbf{C}_2)$ has a minimum rank r over the set of two tuples of distinct code vector sequences, then a diversity rM is achieved.
- Determinant Criterion: The minimum of the r-th roots of the sum of determinants of all $r\times r$ principal cofactors of $\mathbf{A}(\mathbf{C}_1,\mathbf{C}_2)$ taken over all pairs of distinct code vector sequences $\mathbf{C}_1$ and $\mathbf{C}_2$ corresponds to coding gain, r being the rank of $\mathbf{A}(\mathbf{C}_1,\mathbf{C}_2)$. The target of code design is making this sum as large as possible. If a code is designed to give a diversity gain of NM, for a better coding gain, the minimum of the determinant of $\mathbf{A}(\mathbf{C}_1,\mathbf{C}_2)$ taken over all pairs of distinct code vector sequences $\mathbf{C}_1$ and $\mathbf{C}_2$ must be maximized.

Space-Time Block Codes


Signal 2
Constellation Mapper
Information Source
ST Block Code
$[c_1\ c_2] \rightarrow \begin{bmatrix} c_1 & -\bar{c}_2 \\ c_2 & \bar{c}_1 \end{bmatrix}$
Constellation Mapper
Signal 1

- Idea:

$$[c_1 \;\; c_2] \rightarrow \begin{bmatrix} c_1 & -\bar{c}_2 \\ c_2 & \bar{c}_1 \end{bmatrix}$$

- Assumption: channel is quasi-static.

Decoding of STBC

- Received Signal:

$$r_1 = h_1 c_1 + h_2 c_2 + n_1$$

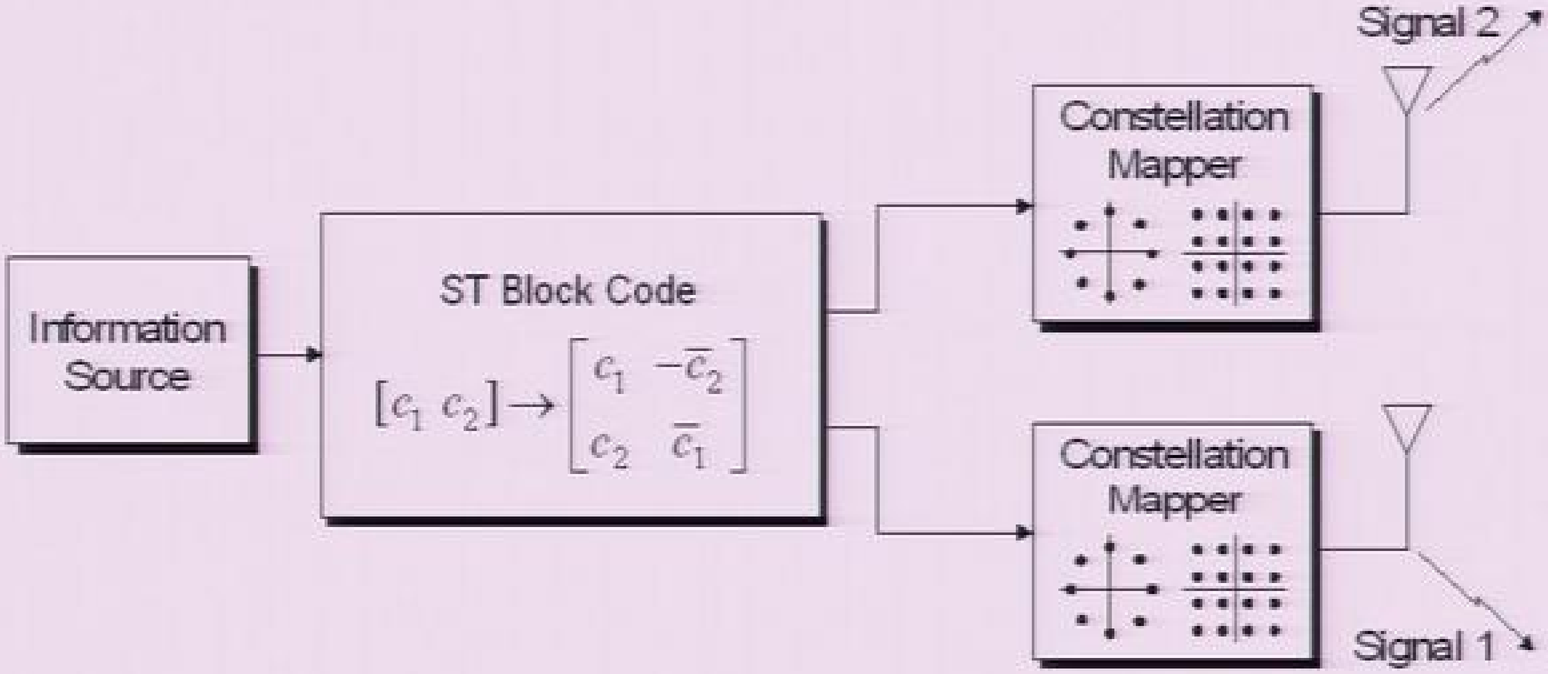
$$r_2 = -h_1 c_2^* + h_2 c_1^* + n_2$$

$$\mathbf{r} = \begin{pmatrix} r_1 \\ r_2^* \end{pmatrix} = \begin{pmatrix} h_1 & h_2 \\ h_2^* & -h_1^* \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} + \begin{pmatrix} n_1 \\ n_2^* \end{pmatrix}$$

- **H** is orthogonal:

$$\mathbf{H}^* \, \mathbf{r} = (\| \mathrm{h}_1 \|^2 + \| \mathrm{h}_2 \|^2) \, \mathbf{c} + \mathbf{H}^*\mathbf{n}$$

Space-Time Block Codes


Information Source
ST Block Code
$[c_1\ c_2] \rightarrow \begin{bmatrix} c_1 & -\overline{c_2} \\ c_2 & \overline{c_1} \end{bmatrix}$
Constellation Mapper
Constellation Mapper
Signal 2
Signal 1

- Idea:

$$[c_1 \;\; c_2] \rightarrow \begin{bmatrix} c_1 & -\overline{c_2} \\ c_2 & \overline{c_1} \end{bmatrix}$$

- Assumption: channel is quasi-static.

Decoding of STBC

- Received Signal:

$$r_1 = h_1 c_1 + h_2 c_2 + n_1$$

$$r_2 = -h_1 c_2^* + h_2 c_1^* + n_2$$

$$\mathbf{r} = \begin{pmatrix} r_1 \\ r_2^* \end{pmatrix} = \begin{pmatrix} h_1 & h_2 \\ h_2^* & -h_1^* \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} + \begin{pmatrix} n_1 \\ n_2^* \end{pmatrix}$$

- **H** is orthogonal:

$$\mathbf{H}^* \, \mathbf{r} = (\| \mathrm{h}_1 \|^2 + \| \mathrm{h}_2 \|^2) \, \mathbf{c} + \mathbf{H}^* \mathbf{n}$$

Real Orthogonal Designs

Definition: Let $u_0, u_1, \ldots, u_{s-1}$ be positive integers, and let $x_0, x_1, \ldots, x_{s-1}$ be commuting indeterminates. A **real orthogonal design** of size N and type $(u_0, u_1, \ldots, u_{s-1})$ is an $N \times N$ matrix X with entries 0, $\pm x_0$, $\pm x_1, \ldots, \pm x_{s-1}$ satisfying

$$XX^T = \left(\sum_{j=0}^{s-1} u_j x_j^2 \right) I_N$$

N = 2, R = 1: This is the representation of the complex numbers as a 2×2 matrix algebra over the real numbers R, where the complex number $x_0 + ix_1$ corresponds to the matrix

$$\begin{pmatrix} x_0 & x_1 \\ -x_1 & x_0 \end{pmatrix}$$

Definition: Rate $R = S/N$

Space-Time Block Codes and Hamilton's Biquaternions

N = 4, R = 1: This is the representation of the quaternions as a 4×4 matrix algebra over R, where the quaternion $x_0 + ix_1 + jx_2 + kx_3$ corresponds to the matrix

$$\left[\begin{array}{cc|cc} x_0 & x_1 & x_2 & x_3 \\ -x_1 & x_0 & -x_3 & x_2 \\ \hline -x_2 & x_3 & x_0 & -x_1 \\ -x_3 & -x_2 & x_1 & x_0 \end{array}\right] = x_0 I + x_1 \left[\begin{array}{cc|cc} & 1 & & \\ -1 & & & \\ \hline & & & -1 \\ & & 1 & \end{array}\right]$$

$$+ x_2 \left[\begin{array}{cc|cc} & & 1 & \\ & & & 1 \\ \hline -1 & & & \\ & -1 & & \end{array}\right] + x_3 \left[\begin{array}{cc|cc} & & & 1 \\ & & -1 & \\ \hline & 1 & & \\ -1 & & & \end{array}\right]$$

Hamilton's Biquaternions: Quaternions as pairs of complex numbers

$$(a,b)(a',b') = (aa' - \overline{b'}b, ab' + \overline{a'}b)$$

$$(a,b) \leftrightarrow \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$$

matrix multiplication = rule for multiplying biquaternions

Complex Orthogonal Designs

Definition: A complex orthogonal design of size N and type $(u_0,\ldots,u_{s-1};v_1,\ldots,v_t)$ is a matrix $Z = X + iY$, where X,Y are real orthogonal designs of type $(u_0,\ldots,u_{s-1})$ and $(v_1,\ldots,v_t)$ respectively, and where

$$ZZ^* = \left(\left(\sum_{j=0}^{s-1} u_j x_j^2\right) + \left(\sum_{j=1}^{t} v_j y_j^2\right)\right) I_N$$

$$\begin{aligned} ZZ^* &= (X + iY)(X^T - iY^T) \\ &= (XX^T + YY^T) + i(YX^T - XY^T) \end{aligned}$$

Hence $XY^T = YX^T$

Definition: Rate $R = (s+t)/2N$

Octonions or Cayley Numbers

View octonions as 4-tuples of complex numbers. Rule for multiplication:

$$
\begin{aligned}
c_0 &= a_0 b_0 - \overline{b_1} a_1 - \overline{b_2} a_2 - \overline{a_3} b_3 \\
c_1 &= b_1 a_0 + a_1 \overline{b_0} - a_3 \overline{b_2} + b_3 \overline{a_2} \\
c_2 &= b_2 a_0 - \overline{a_1} b_3 + a_2 \overline{b_0} + \overline{b_1} a_3 \\
c_3 &= b_3 \overline{a_0} + a_1 b_2 - b_1 a_2 + a_3 b_0
\end{aligned}
$$

Right multiplication of an octonion a by octonions of the form $b = (b_0, b_1, b_2, 0)$:

$$
a \to a \begin{pmatrix} b_0 & b_1 & b_2 & 0 \\ -\overline{b_1} & \overline{b_0} & 0 & b_2 \\ -\overline{b_2} & 0 & \overline{b_0} & -b_1 \\ 0 & -\overline{b_2} & \overline{b_1} & b_0 \end{pmatrix}
$$

Rate 3/4 complex orthogonal design

Hurwitz-Radon Families of Matrices

$$\begin{tikzcd}
X = \sum_{i=0}^{s-1} x_i A_i \arrow[d, dash] \\
B_i = (u_0 u_i)^{-1/2} A_i A_0^T \arrow[d] \\
X = \sum_{i=0}^{s-1} x_i B_i
\end{tikzcd}$$

real orthogonal design of size N and type $(u_0, \ldots, u_{s-1})$

$$A_i A_i^T = u_i I_N$$

$$A_i A_j^T = -A_j A_i^T \quad i \neq j$$

(change of basis)

$$B_0 = I_N$$

$$B_i^T = -B_i$$

$$B_i B_i^T = I_N$$

$$B_i B_j^T = -B_j B_i^T \quad i \neq j$$

The Computer as Physics Experiment

1946 – ENIAC

2001 – NMR Quantum Computer at Los Alamos

NY Times (March 27) Emanuel Knill and Raymond Laflamme at Los Alamos

The Computer as Physics Experiment

1946 – ENIAC

2001 – NMR Quantum Computer at Los Alamos

$$\sum_{v\in V}\alpha_v\,|\,v\rangle,\ V=\mathbf{Z}_2^N \text{ and } \sum_{v\in V}|\,\alpha_v\,|^2=1$$

Quantum Systems

We consider a system with N 2-state memory cells

Classical Physics: this is completely described by N bits

Quantum Physics: this is described by $2^N - 1$ complex numbers

A *quantum bit* or *qubit* is an individual 2-state memory cell — mathematically this is a 2-dim. Hilbert space

$$\alpha \,|\, 0\rangle + \beta \,|\, 1\rangle, \;\; |\, \alpha \,|^2 + |\, \beta \,|^2 = 1$$

N qubits are described mathematically as the tensor product of the individual 2-dim. Hilbert spaces

$$\sum_{v \in V} \alpha_v \,|\, v\rangle, \; V = \mathbf{Z}_2^N \;\text{ and }\; \sum_{v \in V} |\, \alpha_v \,|^2 = 1$$

Superposition, Measurement and the Heisenberg Uncertainty Principle

Superposition: Classical bits take the value 0 or the value 1

Qubits can occupy a superposition of the states 0 and 1

Measurement: Measure the qubit $\alpha|0\rangle+\beta|1\rangle$ wrt. basis $|0\rangle,|1\rangle$

$$\alpha|0\rangle+\beta|1\rangle \rightarrow \begin{cases} |0\rangle & \text{with probability } |\alpha|^2 \\ |1\rangle & \text{with probability } |\beta|^2 \end{cases}$$

No Cloning: Observations of a quantum system, no matter how delicately performed cannot yield complete information on system state before measurement

Quantum Error Correction: Makes it possible to assemble reliable computers out of unreliable components

- Cannot be achieved by duplicating quantum bits

The Error Process

$X(e_i)$ applies the Pauli matrix $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ to the ith qubit and fixes the remaining qubits

- this is a **bit** error in the ith qubit

$Z(e_i)$ applies the Pauli matrix $\sigma_x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ to the ith qubit and fixes the remaining qubits

- this is a **phase** error in the ith qubit

$X(a)\,Z(b)$ produces bit errors in the qubits for which $a_i = 1$ and phase errors in the qubits for which $b_i = 1$

Principle: Any code which corrects these types of quantum errors will be able to correct errors in arbitrary models, assuming the errors are not correlated among large numbers of qubits and that the error rate is small

Quadratic and Bilinear Forms over Z^2

Group E of tensor products $\underline{+}\omega_1 \otimes \ldots \otimes \omega_N$ where each ω_i is

$$I, \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ or } \sigma_x \sigma_z$$

Commutative subgroups are important — look at $N = 5$, and specify 16 commuting matrices of size $2^5 = 32$

$$\sigma_z \otimes \sigma_x \sigma_z \otimes \sigma_x \otimes \sigma_z \otimes I \leftrightarrow \overset{a}{01100} \Big| \overset{b}{11010} \quad X(a)Z(b)$$

$X(a)Z(b)$ commutes with $X(a')Z(b')$ if and only if $a \cdot b' + a' \cdot b = 0$

$$\begin{array}{ccccc|ccccc} & & a & & & & & b & & \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{array}$$

Quantum Error Correction

How it works: the trick is to take quantum superposition + decoherence and to measure the decoherence in a way that gives no information about the original superposition, and then to correct the measured decoherence

S is a group of 2×2^k commuting symmetric matrices $(\pm I)$

$$\begin{tikzcd}
O(\mathrm{R}^{2^N}) \arrow[d, dash] \\
L \arrow[d, dash] \\
E \arrow[d, dash] \\
S
\end{tikzcd}$$

The group $\overline{S}$ has 2^k distinct linear characters each afforded by a 2^{N-k} dim. eigenspace of X^{2^N}. Choose one of these eigenspaces — wlog. the eigenspace R corresponding to the trivial character

Then R is a quantum error-correcting code that encodes N–k qubits into N qubits. The quantum error-correcting properties of R are determined by combinatorial properties of S

Example

Example. A quantum error-correcting code R mapping 1 qubit into 5 qubits

This code contains 2 codewords:

$$\begin{aligned}|c_0\rangle = &|00000\rangle \\ &+|11000\rangle+|01100\rangle+|00110\rangle+|00011\rangle+|10001\rangle \\ &-|10100\rangle-|01010\rangle-|00101\rangle-|10010\rangle-|01001\rangle \\ &-|11110\rangle-|01111\rangle-|10111\rangle-|11011\rangle-|11101\rangle ,\end{aligned}$$

and

$$\begin{aligned}|c_1\rangle = &|11111\rangle \\ &+|00111\rangle+|10011\rangle+|11001\rangle+|11100\rangle+|01110\rangle \\ &-|01011\rangle-|10101\rangle-|11010\rangle-|01101\rangle-|10110\rangle \\ &-|00001\rangle-|10000\rangle-|01000\rangle-|00100\rangle-|00010\rangle\end{aligned}$$

R is fixed by cyclic permutations and by $X(11000)Z(00101)$

R is the eigenspace fixed by the 4-dim. subspace S

Quantum Error Correction

How it works: the trick is to take quantum superposition + decoherence and to measure the decoherence in a way that gives no information about the original superposition, and then to correct the measured decoherence

$$\begin{tikzcd}
O(\mathrm{R}^{2^N}) \arrow[d, dash] \\
L \arrow[d, dash] \\
E \arrow[d, dash] \\
S
\end{tikzcd}$$

S is a group of 2×2^k commuting symmetric matrices $(\pm I)$

The group $\overline{S}$ has 2^k distinct linear characters each afforded by a 2^{N-k} dim. eigenspace of X^{2^N}. Choose one of these eigenspaces — wlog. the eigenspace R corresponding to the trivial character

Then R is a quantum error-correcting code that encodes N–k qubits into N qubits. The quantum error-correcting properties of R are determined by combinatorial properties of S

Quadratic and Bilinear Forms over Z^2

Group E of tensor products $\pm\omega_1 \otimes \ldots \otimes \omega_N$ where each ω_i is

$$I, \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ or } \sigma_x\sigma_z$$

Commutative subgroups are important — look at $N = 5$, and specify 16 commuting matrices of size $2^5 = 32$

$$\sigma_z \otimes \sigma_x\sigma_z \otimes \sigma_x \otimes \sigma_z \otimes I \leftrightarrow \overset{a}{01100} \big| \overset{b}{11010} \ \ X(a)Z(b)$$

$X(a)Z(b)$ commutes with $X(a')Z(b')$ if and only if $a \cdot b' + a' \cdot b = 0$

$$\begin{array}{ccccc|ccccc}
 & & a & & & & & b & & \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0
\end{array}$$

Quantum Error Correction

How it works: the trick is to take quantum superposition + decoherence and to measure the decoherence in a way that gives no information about the original superposition, and then to correct the measured decoherence

$$\begin{tikzcd}
O(\mathrm{R}^{2^N}) \arrow[d, dash] \\
L \arrow[d, dash] \\
E \arrow[d, dash] \\
S
\end{tikzcd}$$

S is a group of 2×2^k commuting symmetric matrices $(\pm I)$

The group $\overline{S}$ has 2^k distinct linear characters each afforded by a 2^{N-k} dim. eigenspace of X^{2^N}. Choose one of these eigenspaces — wlog. the eigenspace R corresponding to the trivial character

Then R is a quantum error-correcting code that encodes N–k qubits into N qubits. The quantum error-correcting properties of R are determined by combinatorial properties of S

Example

Example. A quantum error-correcting code R mapping 1 qubit into 5 qubits

This code contains 2 codewords:

$$
\begin{aligned}
|c_0\rangle = {} & |00000\rangle \\
& + |11000\rangle + |01100\rangle + |00110\rangle + |00011\rangle + |10001\rangle \\
& - |10100\rangle - |01010\rangle - |00101\rangle - |10010\rangle - |01001\rangle \\
& - |11110\rangle - |01111\rangle - |10111\rangle - |11011\rangle - |11101\rangle ,
\end{aligned}
$$

and

$$
\begin{aligned}
|c_1\rangle = {} & |11111\rangle \\
& + |00111\rangle + |10011\rangle + |11001\rangle + |11100\rangle + |01110\rangle \\
& - |01011\rangle - |10101\rangle - |11010\rangle - |01101\rangle - |10110\rangle \\
& - |00001\rangle - |10000\rangle - |01000\rangle - |00100\rangle - |00010\rangle
\end{aligned}
$$

R is fixed by cyclic permutations and by $X(11000)Z(00101)$

R is the eigenspace fixed by the 4-dim. subspace S

Fundamental Upper Bound on the Rate of Real Orthogonal Designs

Theorem (Radon, 1922): Given $N = 2^{4a+b} N_0$, where N_0 is odd, define $\rho(N) = 8a + 2^b$. Then

(1) The size s of a Hurwitz-Radon family is at most $\rho(N) - 1$

(2) There exists a family with exactly $s = \rho(N) - 1$ integer matrices

$(1|1)$

$N - 2$

$(10|10)$

$(11|01)$

$(01|11)$

$N = 4$

$(010|010)$

$(011|001)$

$(001|111)$

$(101|011)$

$(110|101)$

$(111|100)$

$(100|110)$

$N = 8$

skew-symmetric matrices that square to $-I$ and that pairwise anticommute

Complex Designs and Hurwitz-Radon Families of Type (*s*,*t*)

$$Z = X + iY \qquad X = \sum_{i=0}^{s} x_i A_i,\ Y = \sum_{i=1}^{t} y_i B_i$$

$$\big|$$

$$A_i A_i^T = u_i I_N \qquad B_i B_i^T = v_i I_N$$

$$A_i A_j^T = -A_j A_i^T \qquad B_i B_j^T = -B_j B_i^T$$

$$A_i B_j^T = B_j A_i^T$$

$$\alpha_i = (u_0 u_i)^{-1/2} A_i A_0^T$$

$$\beta_j = (u_0 v_j)^{-1/2} B_j A_0^T$$

$$\downarrow$$

$$\alpha_i = -\alpha_i^T \qquad \beta_i = \beta_i^T$$

$$\alpha_i^2 = -I_N \qquad \beta_i^2 = I_N$$

$$\alpha_i \alpha_j = -\alpha_j \alpha_i \qquad \beta_i \beta_j = -\beta_j \beta_i$$

$$\alpha_i \beta_j = -\beta_j \beta_i$$

$$Z = \sum_{i=0}^{s} x_i \alpha_i + \sum_{j=1}^{t} y_j \beta_j$$

These relations define a Clifford Algebra $C^{s,t}$ of type (s,t)

Fundamental Upper Bound on the Rate of Complex Orthogonal Designs

Given t symmetric, anti-commuting orthogonal matrices of size N, let $\rho_t(N)-1$ be the number of skew-symmetric, anti-commuting orthogonal matrices of size N that anti-commute with the given t matrices:

$\rho_t(N) = \max\{s \mid C^{s-1,t}$ has an irreducible matrix representation over 👍 of degree $N\}$

Theorem (Wolfe): There exists an amicable pair X,Y of real orthogonal designs of size N, where X has type $(1,\ldots,1)$ on variables $x_0, x_1, \ldots, x_s$, and Y has type $(1,\ldots,1)$ on variables $y_1,\ldots,y_t$ if and only if $s \le \rho_t(N)-1$

Theorem (Wolfe): Let X,Y be an amicable pair of real orthogonal designs of size $N = 2^h N_0$, where N_0 is odd. Then the total number of variables in X and Y is at most $2h+2$, and this bound is achieved by designs X,Y that each involve $h+1$ variables

4×4 Complex Designs

Number of Variables in Y	Number of Variables in X
t	$\rho_t(4)$
4	0
3	3
2	3
1	3
0	4

The rate 3/4 complex design derived from the Cayley Numbers is optimal

There is a rate 1 real design of size 8, but no rate 1 complex design of size 4