This paper treats a class of codes made possible by restrictions on measurement related to the uncertainty principal. Two concrete examples and some general results are given.

Conjugate Coding *

Stephen Wiesner

Columbia University, New York, N.Y.
Department of Physics

The uncertainty principle imposes restrictions on the capacity of certain types of communication channels. This paper will show that in compensation for this "quantum noise", quantum mechanics allows us novel forms of coding without analogue in communication channels adequately described by classical physics.

---

* Research supported in part by the National Science Foundation.

We will first give two concrete examples of conjugate coding and then proceed to a more abstract treatment.

Example One: A means for transmitting two messages either but not both of which may be received.

The communication channel is a light pipe or guide down which polarized light is sent. Since the information will be conveyed by variations in the polarization, it is essential that the light pipe does not depolarize the light and that all polarizations of light travel with the same velocity and attenuation.

The two messages are rendered into the form of two binary sequences. The transmitter then sends bursts of light at times that we will label T_1, T_2, etc. The amplitude of the bursts is adjusted so that it is unlikely that more than one photon from each burst will be detected at the receiving end of the light pipe.

Before emitting the ith burst (i=1,2 ...), the transmitter chooses one of the two messages in a random manner by flipping a coin or selecting a bit from a table of random numbers. If the first message is chosen, the ith burst is polarized either vertically or horizontally depending on whether the ith digit of the first binary sequence is a zero or a one. If the second message is chosen, the ith burst is polarized in either the right or left-hand circular sense depending on whether the ith digit of the second message is a zero or a one. See Fig. 1, next sheet.

The receiver contains a quarter wave plate and birefringent crystal, or some other analyzer, that separates

POLARIZATION OF i^{th} BURST

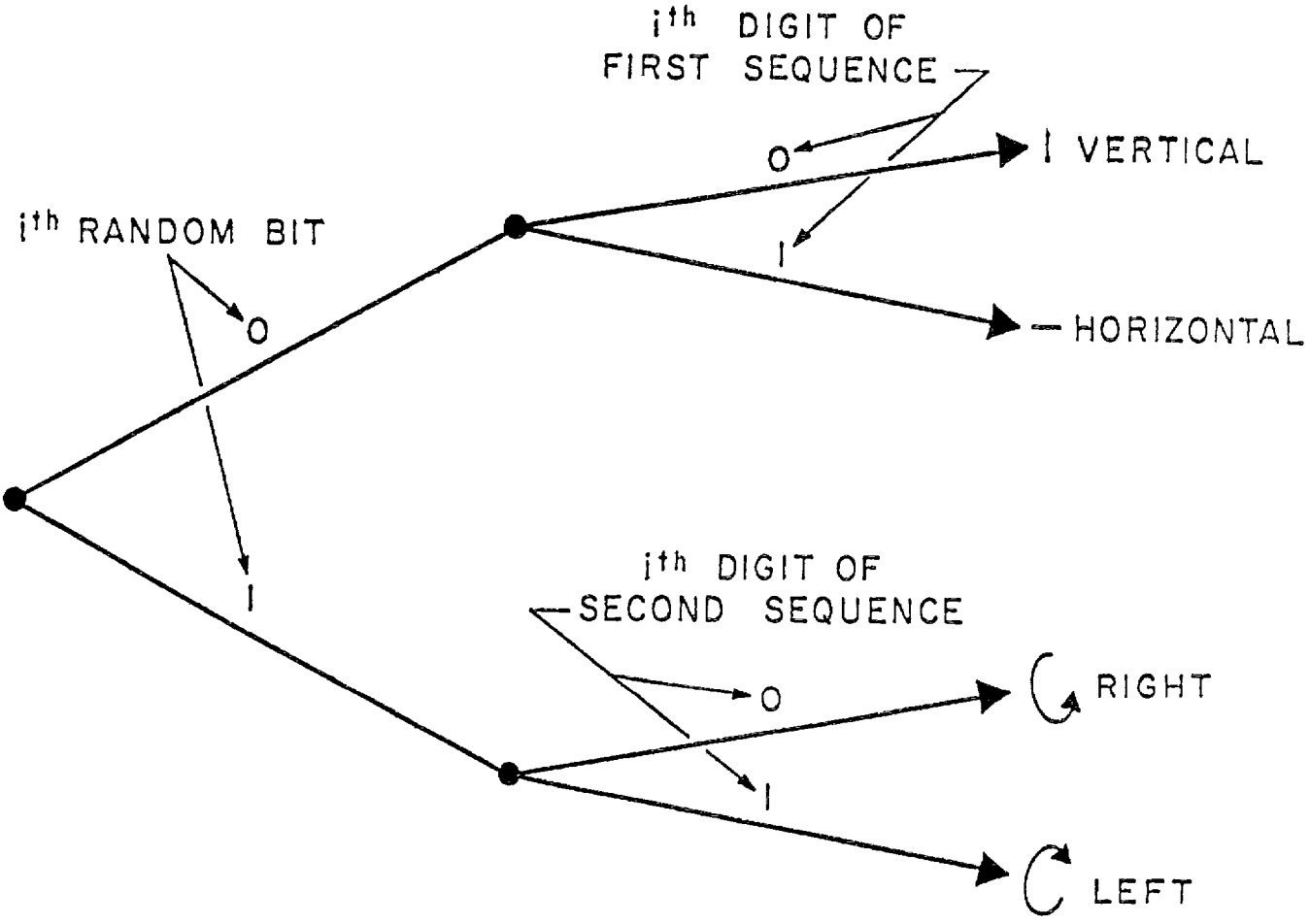

FIG. 1

orthogonally polarized components of the light wave into spatially separate beams. Following this is a pair of the best available photomultiplier tubes. If the first message is to be received, the analyzer is arranged so as to send vertically polarized photons to one phototube and horizontally polarized photons to the other. If the second message is to be received, the separation is made with respect to right and left-hand circular polarization.

Now if the linear polarization of a photon is measured, all chance of measuring its circular polarization is lost. Thus, if the receiver is set to receive the first message, nothing at all is learned about the contents of the second message. Likewise, when the receiver is set to receive the second message, it destroys all information concerning the first message. If the receiver is set up to sort the photons with respect to some elliptical polarizations intermediate between linear and circular, less information about each message is recovered than when the receiver makes the best measurement for the reception of one message alone.

Of course, even when the receiver is set for the first message, a full knowledge of the first sequence is not recovered. In fact, half the digits of the first sequence never even influence the transmitted signal and at the corresponding times, when the second message is being transmitted, the receiver output has an equal probability of being a zero or a one. This noise introduced by the coding scheme, as well as the noise due to the channel, the photon shot noise, and the photomultiplier noise, may be

overcome if an error correcting code of the usual sort is used in forming the binary sequences from the original messages. Care must be taken, for too much redundancy would allow both messages to be recovered by the alternate reception of one sequence and then the other.

There is no way that the receiver can recover the complete contents of more than one of the conjugately coded messages so long as it is confined to making measurements on one burst of photons at a time. In principle, there exist very complicated measurements that allow recovery of all the transmitted information. To see this, consider the transmission of two messages of finite length. The transmitter will produce a signal consisting of a finite number of bursts of polarized light and the entire signal may be described by a single vector ψ in a large Hilbert space spanned by all possible finite transmissions. If one of the messages is changed, a state corresponding to a different vector ψ' is produced. The change from Ψ to Ψ' could be detected unambiguously by a receiver of the type previously described, if set to receive the message that was changed. For this to be possible, Ψ must be orthogonal to Ψ'. It follows that the set $\{\Psi\}$ of the vectors corresponding to all possible pairs of finite messages is ortho-normal and therefore there exists an Hermetian operator or a set of commuting Hermetian operators corresponding to a measurement or measurements that can distinguish all the possible signals.

There is an easy extension to the case of three messages, no two of which may be recovered. One simply transmits a third binary sequence using light in the two polarization states at 45^{o} to vertical and horizontal. Extension to more than three messages is not straight forward.

The above system for sending two mutually exclusive messages could be built at the present time. Though it is possible in principle to beat the system and recover both messages, to do so would require measurements that are completely beyond the reach of present-day technology. The system therefore works in practice but not in principle. The next example is in the opposite category; it is foolproof in principle, but it probably could not be built at the present time.

Example Two: Money that it is physically impossible to counterfeit.

A piece of quantum money will contain a number of isolated two-state physical systems such as, for example, isolated nuclei of spin 1/2. For each two-state system, let a and b represent a pair of ortho-normal base states and let $\alpha = 1/\sqrt{2}(a+b)$ and $\beta = 1/\sqrt{2}(a-b)$ represent another pair.

The two state systems must be well enough isolated from the rest of the universe so that if one of them is initially in the state a or α, there is little chance that a measurement made during the useful lifetime of the money will find it in the orthogonal states b or β, respectively. There is no

device operating at present in which the "phase coherence" of a two-state system is preserved for longer than about a second; however, the continuing advance of cryogenic technique will surely change this.

Let us suppose to be definite that the money contains twenty isolated systems, S_i, i=1, 2, ... 20. At the mint they create two random binary sequences of twenty digits each which we will call M_i and N_i, i=1,2,...20, M_i = 0 or 1, N_i = 0 or 1. Then the two-state systems are placed in one of the four states a, b, α or β in accordance with the scheme shown in Fig. 2.

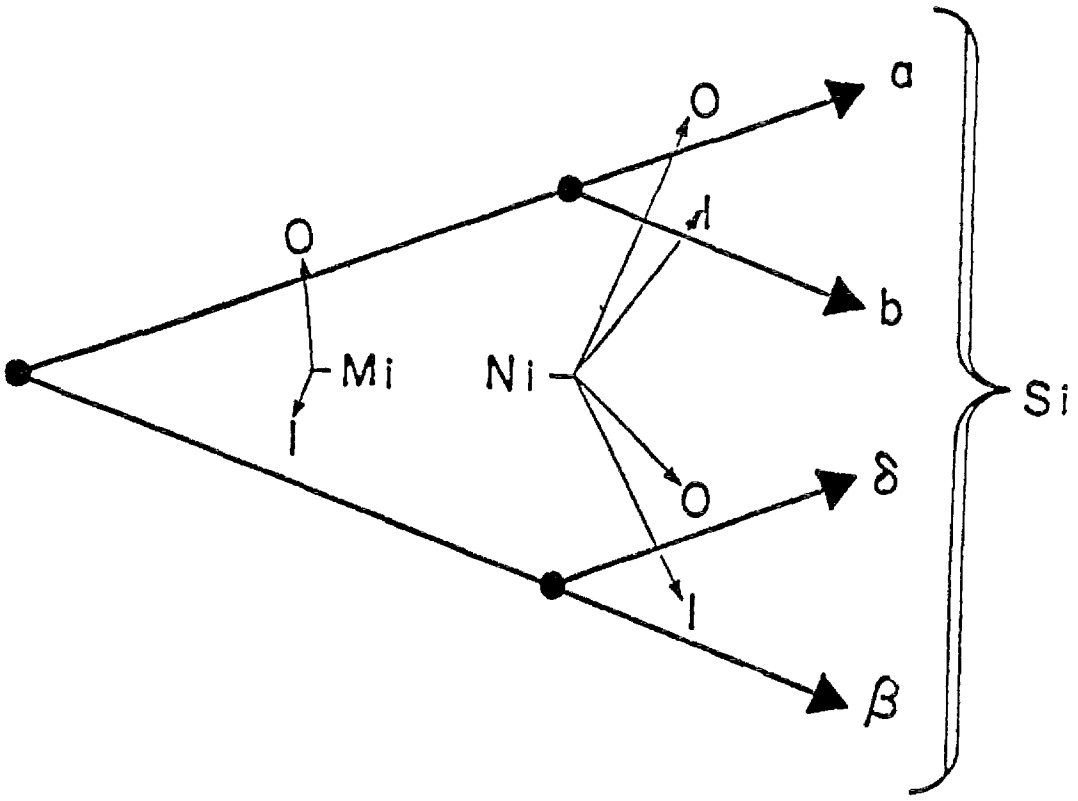

FIG. 2

The money is also given a serial number which is printed on it in the usual way and the two binary sequences

describing its initial state are kept on record at the mint and perhaps at a number of branch banks.

When the money is returned to the mint, a check is made to see if each isolated system is still in its initial state or whether it has switched to the orthogonal state.

Now consider the problem of someone who would duplicate a piece of quantum money. He cannot recover N_i because, since he does not know M_i, he does not know what measurements to make on S_i. A measurement on a particular S_i that distinguishes a from b must necessarily destroy all chance of distinguishing α from β. Likewise a measurement that distinguishes α from β destroys the chance of distinguishing a from b. Suppose a counterfeiter goes ahead anyway, makes some measurement on the S_i and produces money with the new S_i in the states found by his measurements. Then for each i, there is a 50% chance that he will make the wrong measurement and in this event, there is a 50% chance that a measurement at the mint will show S_i to be in the wrong state. Thus, there is a 1/4 chance of each digit being found wrong and the probability of the whole counterfeit coin passing inspection is only $(3/4)^{20} < 0.00317$.

Could there be some way of duplicating the money without learning the sequence N_i? No, because if one copy can be made (so that there are two pieces of the money) then many copies can be made by making copies of copies. Now given an unlimited supply of systems in the same state, that state can be determined. Thus, the sequence N_i could be recovered. But this is impossible.

Conjugate Bases

If the momentum of a particle is known, then nothing is known about its position; in other words, it is equally likely to be found in all regions possessing a fixed volume V. Likewise, if the position is known, then nothing is known about its momentum. The same relation holds between all pairs of conjugate variables and this suggests an extension of the idea of conjugation from variables to basis sets.

Let

$$\{a_i\},\ i=1,2,\ldots,N \text{ and } \{b_i\},\ i=1,\ldots N$$

be two ortho-normal bases for an N dimensional Hilbert space. We call such a pair conjugate if and only if $|(a_i,b_j)|^2 = \frac{1}{N}$ for all i and j.* Physically, if a system is in a state described by a_i, i=1,...,N, then it must have an equal probability of being found in any of the states b_i, i=1,...,N and vice versa, if it is in a state b_i it must have an equal probability to be found in any a_i.

A collection of bases will be called conjugate if each pair of bases in the collection is conjugate. We can now present a definition.

A conjugate code is any communication scheme in which the physical systems used as signals are placed in states corresponding to elements of several conjugate basis of the Hilbert space describing the individual systems. Note that in the case where the sequence of signals has more than one element the above definition does not require the vectors describing entire transmissions to be elements of conjugate base sets. This last condition was fulfilled in the second example but not in the first.

---

* (a_i, b_i) is the inner product $\langle a_i | b_i \rangle$ in the Dirac notation.

In addition to pairs of conjugate bases, there are triplets of conjugate bases. For example, in a two-dimensional system we have

$\{a, b\}$ $\qquad |a|^2=|b|^2=1 \quad (a,b)=0$

$\{1/\sqrt{2}(a+b),\ 1/\sqrt{2}(a-b)\}$

$\{1/\sqrt{2}(a+ib),\ 1/\sqrt{(a-ib)}\}$.

Three such bases were used in the scheme for sending three messages no two of which can be received.

Are there sets bigger than triplets? The following theorem shows that there is no limit to the multiplicity of mutually conjugate basis sets.

Theorem: In an Hilbert space of dimension $2^{(N-1)!/2}$, there exists sets of N mutually conjugate basis sets. Proof: Suppose the theorem to be true for $N \leq M$ // . Let $\{A^\alpha\}$, $\alpha=1...M$ be a set of mutually conjugate ortho-normal basis on an Hilbert space H of dem. $2^{(M-1)!/2} \equiv D$

$$A^\alpha\{a_i{}^\alpha\} \quad i=1 \ldots D$$

and

$$|(a_1{}^\alpha,\ a_j{}^\beta)|^2 = \frac{1}{D}$$

for all $\alpha \neq \beta$.

We can then construct M+1 mutually conjugate bases on the space $H \otimes H \otimes \ldots \otimes H = H^M$. *

For the first M basis, we take a natural extension of the basis sets A^α. Call $\bar{A}^\alpha$ the basis set of H^M consisting of the vectors $a_1{}^\alpha \otimes a_j{}^\alpha \ldots \otimes a_\ell{}^\alpha$, i, j, ... ℓ ... D .

* $\otimes$ is the tensor product. $H \otimes H'$ is defined as the space of all linear functions from H into H'.

Note that is $\alpha \neq \beta$,

$$|(a_i^{\alpha} \otimes \ldots a_{\ell}^{\alpha},\ a_m^{\beta} \otimes \ldots \otimes a_p^{\beta})|^2 = |(a_i^{\alpha}, a_m^{\beta})|^2 \times$$

$$\ldots \times |(a_{\ell}^{\alpha}, a_p^{\beta})|^2 = \left(\frac{1}{D}\right)^M$$

so these basis sets $\{\bar{A}^{\alpha}\}$ are mutually conjugate.

For the last basis, we take the vectors

$$V(q,\{P^{\alpha}\}) = \frac{1}{\sqrt{D}} \sum_{K=1}^{D} e^{2\pi i \frac{qK}{D}} \times a_K^1 \otimes a_{p^2(K)}^2 \cdots \otimes a_{p^M(K)}^M$$

here, $q = 1 \ldots D$ and $\{P^{\alpha}\}$, $\alpha = 2, 3 \ldots M$ is a set of cyclic permutations on the integers $1 \ldots D$. (i.e., $P^{\alpha}(n) = n+J_{\alpha}$ Mod(D) for some integer J_{α}.) Call this last basis V.

Since there are D cyclic permutations on D intergers, there are D^{M-1} sets $\{P^{\alpha}\}$ and $DxD^{M-1} = D^M$ vectors $V(q,\{P^{\alpha}\})$ in V; as there should be.

The proof that V is ortho-normal is obvious.

So, actually, is the proof that V is conjugate to the other basis sets, but I give it since it is the heart of the matter. Fix α and let $W \equiv a_i^{\alpha} \otimes \ldots \otimes a_{\ell}^{\alpha}$ be a typical vector of A_{α}. Then

$$|(W, V(q,\{P^{\alpha}\}))|^2 = \frac{1}{D}\left| \sum_{K=1}^{D} e^{2\pi i \frac{qK}{D}} \times (a_i^{\alpha} \otimes \ldots a_{\ell}^{\alpha}, a_K^1 \otimes \ldots a_{p^M(K)}^M)\right|$$

The inner product will be zero unless $a_{p^{\alpha}(K)}^{\alpha}$ equals the αth term of W. (Let P^1 be the identity.) This happens for just one value of K, call it k. Then $|(W, V(q,\{P^{\alpha}\}))|^2 =$ $1/D|(a_i^{\alpha} \otimes \ldots a_{\ell}^{\alpha},\ a_k' \otimes \ldots a_{p^M(k)}^M)|^2$

where the αth vector is the same on both sides of the inner product. As for the rest, $|(a_i^{\alpha},\ a^{\beta}p^{\beta}_{(k)})|^2 = 1/D$