denote the table of the i-shortened code for each i. We notice that if $\Pi \in_i H$ and $\Pi(k)=l$, then $\text{Table}_n^i(k)=\text{Table}_n^i(l)$. Furthermore, if there is an m such that $\text{Table}_n^i(m)\neq\text{Table}_n^i(\nu)$ for every ν, then $\Pi\in_m H$ and $\text{Table}_n^m(k)=\text{Table}_n^m(l)$. With the computer we found the tables and from them we found that $\theta({}_iH)=1$. This was done finding an m[6] for which $\text{Table}_n^m(k)\neq\text{Table}_n^m(l)$ whenever $\text{Table}_n^i(k)=\text{Table}_n^i(l)$. In this way we found $\theta(H)$ and concluded that $\theta(G_l^k)=\theta(H_l^k)$ and therefore $G_l^k=H_l^k$. There is one exception: H_1^4 (the group for X^4+X+1) has an extra symmetry, that given by the transposition (i,j) where i,j are the positions corresponding to the field elements 0, 1. This comes from having a codeword with weight two in the dual code.

Acknowledgment

The author wishes to thank the referees for their careful reading, comments, and suggestions which have helped greatly in improving the presentation of these results.

References

[1] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.

[2] ——, "Goppa Codes," *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 590–592, Sept. 1973.

[3] E. R. Berlekamp and O. Moreno, "Extended double error correcting binary Goppa codes are cyclic," *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 817–818, Nov. 1973.

[4] E. R. Berlekamp, H. Rumsey, and G. Solomon, "On the solution of algebraic equations over finite fields," *Inf. Contr.*, vol. 10, pp. 553–564, 1967.

[5] V. D. Goppa, "A new class of linear error-correcting codes," *Probl. Peredach. Inform.*, vol. 6, no. 3, pp. 24–30, Sept. 1970.

[6] ——, "Rational representation of codes and (L,g) codes," *Probl. Peredach. Inform.*, vol. 7, no. 3, pp. 41–49, Sept. 1971.

[7] O. Moreno, "Some properties of Goppa codes," Ph.D. dissertation, Univ. of Calif. at Berkeley, Berkeley, CA, Nov. 1973.

[8] N. J. A. Sloane, "A survey of constructive coding theory," *Discrete Math.* vol. 3, pp. 265–294, Sept. 1972.

[9] R. Hartshorne, *Foundations of Projective Geometry*. New York: W. A. Benjamin, 1967.

[6] m must have the property $\text{Table}_n^i(m)\neq\text{Table}_n^i(k)$ for every k.

Optimum Linear Coding in Continuous-Time Communication Systems with Noisy Side Information at the Decoder

TANGÜL Ü. BAŞAR, MEMBER, IEEE, AND TAMER BAŞAR, SENIOR MEMBER, IEEE

***Abstract*—The problem of optimal coding in a communication system with a noiseless feedback link and with noisy side information at the decoder is treated. The message is taken as a Gaussian random variable and both the main and the side channels are assumed to be continuous white-Gaussian. A linear encoding–decoding scheme is developed which attains the well-known performance bounds for the special cases of i) noiseless side information and ii) no side information.**

I. Introduction

In this correspondence we consider the problem of optimal coding in a communication system with a noiseless feedback link and with noisy side information at the receiver. Both channels are assumed to be continuous and white-Gaussian, and the feedback channel is taken to be noise-free. The message to be transmitted is a Gaussian random variable, and the transmission interval is taken as T s. A similar problem, but in discrete time, has been considered in [1] where the authors have proposed an *ad hoc* linear encoding–decoding scheme which does not asymptotically achieve the known performance bound for the case when the side information is transmitted noise-free. In a recent note [2] they have improved on this scheme by considering the case when the transmitter can also use the side information, and have shown within this context the optimal linear scheme then achieves the said performance bound under noise-free side information. In this correspondence, however, we obtain a solution for the continuous-time version of the problem with noisy side information at the receiver and show that our optimal linear scheme asyptotically achieves the well-known performance bounds in the cases when i) the side information is transmitted to the receiver noise-free, and ii) there is no side information. For the general case, the optimal linear encoder–decoder transformations are obtained in closed form.

In the next section we formulate the problem and give the solution in Section III. Section IV is devoted to a discussion of the asymptotic behavior of the communication system.

Manuscript received March 22, 1978; revised August 22, 1978.

T. Ü. Başar is with the Department of Electrical Engineering, Twente University of Technology, Enschede, The Netherlands.

T. Başar is with the Department of Applied Mathematics, Twente University of Technology, Enschede, The Netherlands, on leave from the Applied Mathematics Division, Marmara Research Institute, Gebze, Kocaeli, Turkey.

II. Formulation of the Problem

Let the source output be denoted by a Gaussian random variable x with mean zero and variance σ_x^2. It is to be transmitted through a continuous-time additive Gaussian white noise channel which is to be used for T s. The source output is first modulated with a time function

$$\ell(t)=\begin{cases}1, & \text{for } 0\leqslant t\leqslant T,\\ 0, & \text{otherwise,}\end{cases} \tag{1}$$

and is then encoded appropriately and transmitted through the channel. It is further assumed that there is a noiseless feedback link from the receiver to the transmitter and that the receiver is provided with noisy side information correlated with x. This side information is also transmitted through a continuous-time additive white-Gaussian noise channel, the output of which is appropriately decoded and sent to the receiver.

As depicted in Fig. 1, the main and the side channel noise processes are denoted by $\sigma_v dv_t/dt$ and $\sigma_w dw_t/dt$, respectively, where v_t and w_t are independent standard Wiener processes defined in the interval $[0,T]$. The side information y_t is characterized as the sum $y_t=(x+u)\ell(t)$, where u is a Gaussian random variable with mean zero, variance σ_u^2, and independent of x. The encoder is assumed to apply a linear transformation to its input; specifically, if the output of the receiver is denoted by r_t at time t, then the output of the encoder at time t is given by

$$\xi_t=A(t)[x_t-r_t] \tag{2a}$$

subject to the input power constraint to the channel

$$E\left[\xi_t^2\right]\leqslant P, \tag{2b}$$

where $x_t \triangleq x\cdot\ell(t)$.

The two decoders, on the other hand, are considered as appropriate causal (measurable) transformations on their input, with the decoder of the main channel satisfying a linear growth property. That is, we assume that $B_t(\zeta_s, s\leqslant t)$ grows at most linearly with $\sup_{0\leqslant s\leqslant t}|\zeta_s|$, where ζ_s is defined by

$$\zeta_s=\int_0^s \xi_\tau\, d\tau+\sigma_v v_s=\int_0^s A(\tau)[x-r_\tau]\, d\tau+\sigma_v v_s. \tag{3a}$$

No such restriction has to be imposed on the other decoder $C_t(\cdot)$ whose input is the Gaussian process

$$z_s=\int_0^s y_\tau\, d\tau+\sigma_w w_s=(u+x)s+\sigma_w w_s. \tag{3b}$$

The output of the receiver is the stochastic process r_t, statisfying

$$r_t=B_t(\zeta_s, s\leqslant t)+C_t(z_s, s\leqslant t), \tag{3c}$$

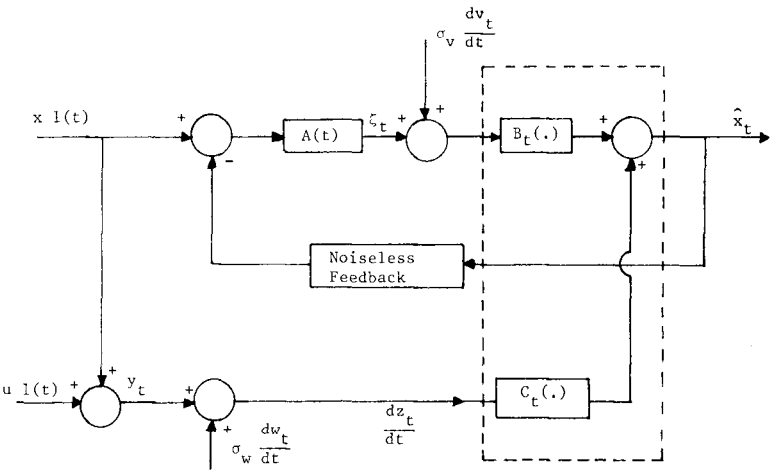

Fig. 1. Schematic diagram of communication system with noisy side information at receiver.

where ζ_s implicity depends on $\{r_\tau, \tau \leqslant s\}$ through (3a). The linear growth property imposed on $B_t(\cdot)$ insures that (3c) admits a unique solution.

The problem considered in this correspondence is now to minimize the quadratic distortion measure

$$D_T = E\left[(r_T - x)^2\right] \tag{4}$$

over all admissible $A(t)$, $B_t(\cdot)$, and $C_t(\cdot)$, and subject to (2b). It will be shown below that this problem admits a unique solution, with the optimal forms of $B_t(\cdot)$ and $C_t(\cdot)$ being linear integral transformations.

III. Derivation of Optimal Encoder and Decoder Transformations

Let $\mathcal{Y}_t$ denote the collection of observations $(\zeta_s, z_s; s \leqslant t)$ where ζ_s and z_s are defined by (3a) and (3b). Introduce the stochastic process

$$\tilde{\zeta}_s = \int_0^s A(\tau) x \, d\tau + \sigma_v v_s, \tag{5}$$

and let $\tilde{\mathcal{Y}}_t$ denote the collection of observations $(\tilde{\zeta}_s, z_s; s \leqslant t)$. It should be noted that $\tilde{\mathcal{Y}}_t$ does not depend on the decoder transformations $\{B_s(\cdot), C_s(\cdot); s \leqslant t\}$, whereas $\mathcal{Y}_t$ does. It has, however, been shown in the Appendix that $\tilde{\mathcal{Y}}_t$ and $\mathcal{Y}_t$ generate the same sigma-field for every admissible pair of decoder transformations. This implies that, for each fixed $A(t)$, (4) is minimized uniquely by the conditional mean $\hat{x}_T = E[x|\tilde{\mathcal{Y}}_T]$, i.e., $r_T = \hat{x}_T$. But since $\tilde{\zeta}_s$ and z_s are linear functions of x, u, v_s, and w_s, and the underlying statistics are Gaussian, $\hat{x}_T$ can be determined as the output of an appropriate Kalman–Bucy filter, which in turn implies that the output of the receiver r_t has to be equal to $r_t = \hat{x}_t \equiv E[x|\tilde{\mathcal{Y}}_t] = E[x|\mathcal{Y}_t]$, where the last equality follows from the equivalence of the sigma-fields generated by $\tilde{\mathcal{Y}}_t$ and $\mathcal{Y}_t$. Hence to determine the optimal decoder transformations for each fixed $A(\cdot)$, we simply substitute $r_\tau = \hat{x}_\tau$ in (3a) and seek to obtain a stochastic differential equation for $\hat{x}_t = E[x|\mathcal{Y}_t]$. To this end, let

$$q_t \triangleq (x\ell(t), u\ell(t))',$$
$$\eta_t \triangleq (\zeta_t, z_t)', \qquad 0 \leqslant t \leqslant T.$$

Then q_t and η_t satisfy the stochastic differential equations

$$dq_t = 0, \qquad q_0 = (x, u)', \tag{6a}$$

$$d\eta_t = H(t) q_t dt - (A(t), 0)' \hat{x}_t dt + G(t) d\epsilon_t, \qquad \eta_0 = 0, \tag{6b}$$

with

$$H(t) \triangleq \begin{pmatrix} A(t) & 0 \\ 1 & 1 \end{pmatrix} \qquad G \triangleq \begin{pmatrix} \sigma_v & 0 \\ 0 & \sigma_w \end{pmatrix} \tag{6c}$$

$$\epsilon_t \triangleq (v_t, w_t)'. \tag{6d}$$

Using this notation $\hat{x}_t$ can be written as

$$\hat{x}_t = (1, 0) E[q_t|\mathcal{Y}_t] \tag{7a}$$

where $\hat{q}_t = E[q_t|\mathcal{Y}_t]$ is given recursively (from the Kalman–Bucy filter theory [3]) by

$$d\hat{q}_t = K(t)[d\eta_t + (A(t), 0)' \hat{x}_t dt - H(t)\hat{q}_t dt], \qquad \hat{q}_0 = 0, \tag{7b}$$

$$K(t) = \Sigma(t) H'(t) [GG']^{-1}, \tag{7c}$$

$$\frac{d\Sigma(t)}{dt} = -\Sigma(t) H'(t) [GG']^{-1} H(t) \Sigma(t), \qquad \Sigma(0) = \operatorname{diag}(\sigma_x^2, \sigma_u^2). \tag{8}$$

The covariance equation (8) admits the unique solution

$$\Sigma(t) = \frac{1}{\Theta(t)} \begin{bmatrix} \frac{t}{\sigma_w^2} + \frac{1}{\sigma_u^2} & -\frac{t}{\sigma_w^2} \\ -\frac{t}{\sigma_w^2} & \frac{t}{\sigma_w^2} + \frac{1}{\sigma_x^2} + \frac{1}{\sigma_v^2} \int_0^t A^2(s)\, ds \end{bmatrix} \tag{9a}$$

where

$$\Theta(t) = \left(\frac{t}{\sigma_w^2} + \frac{1}{\sigma_u^2}\right)\left(\frac{1}{\sigma_x^2} + \frac{1}{\sigma_v^2}\int_0^t A^2(s)\, ds\right) + \frac{t}{\sigma_u^2 \sigma_w^2}. \tag{9b}$$

Hence, for each fixed $A(\cdot)$, the minimum of (4) over admissible decoder transformations is given by

$$D_T = \Sigma_{11}(T) = \left(\frac{T}{\sigma_w^2} + \frac{1}{\sigma_u^2}\right) \Big/ \Theta(T), \tag{10}$$

and the power constraint (2b) can be written as

$$E\left[\xi_t^2\right] = A^2(t)\left[E(x_t - \hat{x}_t)^2\right] = A^2(t) D_t$$
$$= \frac{A^2(t)}{\Theta(t)}\left(\frac{t}{\sigma_w^2} + \frac{1}{\sigma_u^2}\right) \leqslant P. \tag{11}$$

e now have to minimize D_T over $A(\cdot)$ under the constraint (11), which is equivalent to solving the equation

$$\frac{A^2(t)}{\Theta(t)}\left[\frac{t}{\sigma_w^2} + \frac{1}{\sigma_u^2}\right] = P. \tag{12}$$

This integral equation can be written in the form of a differential equation

$$\frac{d}{dt} A^2(t) = \frac{P}{\sigma_v^2} A^2(t) + \frac{P\sigma_w^2}{(\sigma_w^2 + t\sigma_u^2)^2}, \qquad A^2(0) = \frac{P}{\sigma_x^2}, \tag{13}$$

whose solution is

$$[A^*(t)]^2 = \frac{P}{\sigma_x^2}\exp\left(Pt/\sigma_v^2\right) + \int_0^t \exp\left(\frac{P(t-\tau)}{\sigma_v^2}\right)\frac{P\sigma_w^2}{\left(\sigma_w^2+\tau\sigma_u^2\right)^2}\,d\tau. \tag{14}$$

By evaluating the second term of (14) from integral tables, we can also express $A^*(t)$ as the convergent limit of an infinite sequence—a form which we will have occasion to use in Section IV:

$$\begin{aligned}[A^*(t)]^2 = &\left(\frac{1}{\sigma_x^2}+\frac{1}{\sigma_u^2}\right)P\exp\left(\frac{Pt}{\sigma_v^2}\right) - \frac{P}{\sigma_u^2}\cdot\frac{\sigma_w^2}{\sigma_w^2+\sigma_u^2 t}\\ &+\exp\left(Pt/\sigma_v^2\right)e^{-\alpha}\Big[\log\beta(t)+\alpha[\beta(t)-1]\\ &+\frac{\alpha^2}{2.2!}[\beta^2(t)-1]+\frac{\alpha^3}{3.3!}[\beta^3(t)-1]+\cdots\Big]\alpha P/\sigma_u^2\end{aligned} \tag{15}$$

where

$$\alpha \triangleq -P\sigma_w^2/\sigma_v^2\sigma_u^2, \tag{16a}$$

$$\beta(t) \triangleq 1+\frac{\sigma_u^2}{\sigma_w^2}t. \tag{16b}$$

This defines the unique encoder transformation. The corresponding decoder transformation pair, on the other hand, can readily be observed from (7a) and (7b) to be linear integral transformations. One way of determining the explicit forms for optimal $B_t(\cdot)$ and $C_t(\cdot)$ is to solve for $\hat{x}_t$ from (7) in terms of $(\zeta_s, s\leqslant t)$ and $(z_s, s\leqslant t)$ by also making use of the optimum choice for $A(t)$ as given by (14). However, such an approach leads to rather cumbersome mathematical analysis, requiring several nontrivial integrations by parts. Another approach, which is considerably simpler, is to obtain the linear integral transformations by making use of the "orthogonality principle" of the estimation theory. To this end, we first introduce the process

$$\psi_t = \int_0^t A(s)x\,ds + \sigma_v v_t = \zeta_t + \int_0^t A(s)\hat{x}_s\,ds, \tag{17a}$$

and note that the sigma-fields generated by $(\psi_s, z_s, s\leqslant t)$ and $(\zeta_s, z_s, s\leqslant t)$ are the same. Thus the conditional estimate $\hat{x}_t$ can be expressed as

$$\hat{x}_t = E[x|\psi_s, z_s, s\leqslant t]. \tag{17b}$$

Since $\hat{x}_t$ is a linear function of $(\zeta_s, z_s, s\leqslant t)$, it follows from (17) that it is also linear in the new data, which we write as

$$\hat{x}_t = \int_0^t M(t,s)\,d\psi_s + \int_0^t N(t,s)\,dz_s, \tag{17c}$$

where $M(\cdot,\cdot)$ and $N(\cdot,\cdot)$ are kernels yet to be determined. Since the error $\hat{x}_t - x$ is independent of ψ_s, z_s for all $s\leqslant t$, we obtain the two equations

$$\sigma_x^2 A(\tau)\left[\int_0^t N(t,s)\,ds + \int_0^t M(t,s)A(s)\,ds - 1\right] + \sigma_v^2 M(t,\tau) = 0, \tag{18a}$$

$$\sigma_x^2\left[\int_0^t N(t,s)\,ds + \int_0^t M(t,s)A(s)\,ds - 1\right] + \sigma_u^2\int_0^t N(t,s)\,ds + \sigma_w^2 N(t,\tau) = 0, \tag{18b}$$

which should be satisfied for all $\tau\leqslant t$. These integral equations can be shown to admit a solution in the form

$$M(t,s) = L(t)A(s), \tag{19a}$$

$$N(t,s) = \left[\sigma_v^2/\left(\sigma_w^2+t\sigma_u^2\right)\right]L(t), \tag{19b}$$

where

$$L(t) = \sigma_x^2\left[\sigma_x^2\int_0^t A^2(s)\,ds + \sigma_x^2\sigma_v^2 t\left(\sigma_w^2+t\sigma_u^2\right)^{-1} + \sigma_v^2\right]^{-1}. \tag{19c}$$

In particular, if $A(t)$ is given by (14) (the optimal value), we have

$$L^*(t) = P/\sigma_v^2[A^*(t)]^2, \tag{19d}$$

and substitution of this expression, together with (19a)–(19b), into (17c) yields

$$\hat{x}_t = \left(P/\sigma_v^2[A^*(t)]^2\right)\int_0^t A(s)\,d\psi_s + \frac{P[A^*(t)]^{-2}}{\sigma_w^2+t\sigma_u^2}\int_0^t dz_s.$$

Furthermore, if we make use of (17a), we obtain the integral equation

$$\hat{x}_t = \frac{P}{\sigma_v^2[A^*(t)]^2}\left[\int_0^t A^*(s)\,d\zeta_s + \int_0^t [A^*(s)]^2\hat{x}_s\,ds + \frac{\sigma_v^2}{\sigma_w^2+t\sigma_u^2}\int_0^t dz_s\right]$$

which can also be written as a stochastic differential equation

$$\begin{aligned}d\left([A^*(t)]^2\hat{x}_t\right) = &\left(P/\sigma_v^2\right)\left[A^*(t)d\zeta_t + [A^*(t)]^2\hat{x}_t dt\right]\\ &+ P/\left(\sigma_w^2+t\sigma_u^2\right)dz_t + Pz\frac{d}{tdt}\left[1/\left(\sigma_w^2+t\sigma_u^2\right)\right]dt,\end{aligned}$$

admitting the unique solution

$$\begin{aligned}\hat{x}_t = &\left(P/(A^*(t))^2\sigma_v^2\right)\Big[e^{P\sigma_v^{-2}t}\int_0^t e^{-P\sigma_v^{-2}s}A^*(s)\,d\zeta_s\\ &+\int_0^t\left[Pe^{P\sigma_v^{-2}t}F(t,s) + \sigma_v^2/\left(\sigma_w^2+t\sigma_u^2\right)\right]dz_s\Big]\\ \equiv &B_t(\zeta_s, s\leqslant t) + C_t(z_s, s\leqslant t),\end{aligned} \tag{20a}$$

where

$$F(t,s) = \int_s^t\left[e^{-P\sigma_v^{-2}\tau}/\left(\sigma_w^2+\tau\sigma_u^2\right)\right]d\tau. \tag{20b}$$

We have thus completed the proof of our main theorem.

Theorem 1: For the communication system with side information formulated in Section II and depicted in Fig. 1, there exists a unique encoder–decoder triple with the optimal encoder transformation $A^*(t)$ being given by (14) (or (15)). The corresponding optimal decoder transformations are given by

$$B_t^*(\zeta_s, s\leqslant t) = \frac{P}{\sigma_v^2[A^*(t)]^2}e^{P\sigma_v^{-2}t}\int_0^t e^{-P\sigma_v^{-2}s}A^*(s)\,d\zeta_s, \tag{21a}$$

$$C_t^*(z_s, s\leqslant t) = \frac{P}{[A^*(t)]^2}\left[\frac{z_t}{\sigma_w^2+t\sigma_u^2} + P\sigma_v^{-2}e^{P\sigma_v^{-2}t}\int_0^t F(t,s)\,dz_s\right], \tag{21b}$$

where $F(\cdot,\cdot)$ is defined by (20b). The minimum distortion at the receiver (after T s) is given by

$$D_T^* = \Sigma_{11}^*(T) = P/A^*(T). \tag{21c}$$

Remark 1: From an implementation point of view, it might sometimes be simpler to generate the solution of the stochastic differential equation (7b) at the output of the decoders, as compared to designing the two decoders whose mathematical input–output relations are given by (21a) and (21b). In order to achieve this objective, we replace the two decoders (the region inside the dotted lines in Fig. 1) by the two-dimesional system depicted in Fig. 2, whose inputs are $(\zeta_t, z_t, 0\leqslant t\leqslant T)$ and output is $\hat{x}_t$. The quantities K_{ij}^* used in the figure are the entries of $K(t)$ defined by (7c) and (9a), but with $A(\cdot)$ replaced by $A^*(\cdot)$. The relevant expressions for these entries are

$$K_{11}^*(t) = P/\left[\sigma_v^2 A^*(t)\right],$$

$$K_{12}^*(t) = P/\left[A^{*2}(t)\left(t\sigma_u^2+\sigma_w^2\right)\right],$$

$$K_{21}^*(t) = \left(\sigma_u^2/\sigma_v^2\right)A^*(t)K_{12}^*(t),$$

$$K_{22}^*(t) = \sigma_u^2 K_{12}^*(t)\left[\frac{1}{\sigma_x^2} + \frac{1}{\sigma_v^2}\int_0^t A^{*2}(s)\,ds\right].$$

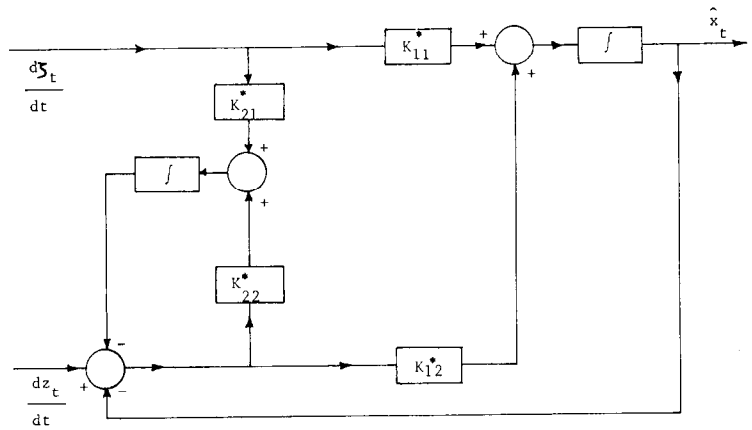

Fig. 2. Optimal replacement of region inside dotted lines in Fig. 1.

IV. Asymptotic Performance Comparison for Small and Large Noise Intensity on the Side Channel

When the transmission of the side information is through a perfect noiseless channel (i.e., when $\sigma_w = 0$), then the optimum achievable performance of the communication system of Fig. 1 can be determined by making use of a recent result of Wyner and Ziv [4]. The rate-distortion function for the source x with the side information $y = x + u$ at the decoder and under the mean-squared error criterion is shown in [4] to be

$$R(D) = \max\left[0, \frac{1}{2}\log_e \frac{\sigma_x^2\sigma_u^2}{(\sigma_x^2+\sigma_u^2)D}\right]. \tag{22a}$$

On the other hand, the channel capacity of the Gaussian white-noise channel with feedback and under the power constraint

$$\int_0^T E[\xi_t^2]\, dt \leqslant PT$$

is (from [5])

$$C(P) = \frac{PT}{2\sigma_v^2} \quad \text{nats.} \tag{22b}$$

Equating (22a) to (22b) we obtain the optimum performance relation

$$D = \frac{\sigma_x^2\sigma_u^2}{\sigma_x^2+\sigma_u^2}\exp\left(-PT/\sigma_v^2\right). \tag{23}$$

This is of course also an upper bound on the performance of our system with additive noise in the side channel. This upper bound will in general not be achievable if $\sigma_w^2 > 0$. However, we can compare the performance of our encoder–decoder design with that given by (28) when $0 < \sigma_w^2 \ll T$, that is, when the noise intensity is sufficiently low but not exactly zero. The reason why we cannot let $\sigma_w^2 = 0$ is because then the Kalman–Bucy filtering theory is not valid (since in deriving the results of Section III we had to assume GG' to be invertible, which is violated if $\sigma_w^2 = 0$). It is possible to circumvent this difficulty by employing generalized Kalman–Bucy filter equations which involve observers, but this will not be pursued here. We will instead show that the bound (23) is asymptotically achieved by our encoder–decoder design as the noise intensity approaches zero.

To this end, we start with expression (21c) and the optimal choice for $A(T)$ which is given by (15). For sufficiently small σ_w^2, (15) yields

$$[A_0^*(T)]^2 \sim \left(\frac{1}{\sigma_x^2} + \frac{1}{\sigma_u^2}\right) P \exp\left(PT/\sigma_v^2\right), \tag{24}$$

and if this is substituted into (21c) we obtain

$$(D_T^*)_0 \to \frac{\sigma_x^2\sigma_u^2}{\sigma_x^2+\sigma_u^2}\exp\left(-PT/\sigma_v^2\right), \tag{25}$$

which verifies that for sufficiently small σ_w^2 the overall performance of our system is optimal within the class of all causal encoder–decoder triples.

Another extreme case is when there is no side information at the decoder, i.e., when $\sigma_w^2 \to \infty$. Going back to expression (14), we note that in this case

$$[A^*(T)]_\infty^2 \to \frac{P}{\sigma_x^2}\exp\left(PT/\sigma_v^2\right), \tag{26}$$

and thus the distortion becomes

$$(D_T^*)_\infty \to \sigma_x^2 \exp\left(-PT/\sigma_v^2\right), \tag{27}$$

which is identical with the overall optimal performance achievable in this case (see [6]).

We see that the encoder–decoder triple given in Theorem 1 achieves the well-known bounds for the two extreme cases. It is conceivable that the given designs are also optimal in the mid-ranges of the noise intensity. But since the rate-distortion function has not yet been obtained for this case, a justification of this conjecture is not readily available.

Acknowledgment

We would like to thank an anonymous reviewer for some very helpful suggestions, in particular, with regard to the derivation of (21).

Appendix

In this Appendix we prove that the sigma-fields generated by $\mathcal{Y}_t = (\zeta_s, z_s; s \leqslant t)$ and $\tilde{\mathcal{Y}}_t = (\tilde{\zeta}_s, z_s; s \leqslant t)$ are the same for all permissible decoder transformations $B(\cdot)$, $C(\cdot)$, and for a fixed encoder transformation $A(\cdot)$. This result will be achieved by verifying the existence of a causal and causally invertable transformation between $\mathcal{Y}_t$ and $\tilde{\mathcal{Y}}_t$. Let us first note from (3a) and (5) the relation

$$\tilde{\zeta}_t = \zeta_t + \int_0^t A(\tau) r_\tau\, d\tau$$

which together with (3c) proves that $\tilde{\mathcal{Y}}_t$ can be expressed in terms of $\mathcal{Y}_s$, $s \leqslant t$ by a measurable transformation. To verify the reverse transformation let us start with (3a), writing it in the form

$$d\zeta_s = -A(s)[B_s(\zeta_\tau, \tau \leqslant s)]ds - A(s)[C_s(z_\tau, \tau \leqslant s)]ds + d\tilde{\zeta}_s, \quad \zeta_0 = 0,$$

which is a stochastic differential equation for ζ_s. But under the linear growth condition on $B_s(\cdot)$, it admits a unique solution ζ_t which clearly depends on $\tilde{\mathcal{Y}}_s$, $s \leqslant t$ through a measurable causal transformation.

References

[1] H. Sakai, T. Soeda, and H. Tokumaru, "A Note on feedback communication with noisy side information at the decoder," *IEEE Trans. Inform. Theory*, vol. IT-23, no. 3, pp. 384–387, May 1977.

[2] H. Sakai, T. Soeda, and H. Tokumaru, "Optimal linear coding schemes for feedback communication with noisy side information," *IEEE Trans. Inform. Theory*, vol. IT-24, no. 3, pp. 381–384, May 1978.

[3] R. E. Kalman and R. S. Bucy, "New results in linear filtering and prediction theory", *ASME Trans., J. Basic Eng.*, vol. 83D, pp. 95–108, 1961.

[4] A. D. Wyner and J. Ziv, "The rate-distortion function for the source coding with side information at the decoder," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 1–10, Jan. 1976.

[5] T. T. Kadota, M. Zakai, and J. Ziv, "Capacity of a continuous memoryless channel with feedback," *IEEE Trans. Inform. Theory*, vol. IT-17, no. 4, pp. 372–378, July 1971.

[6] S. Ihara, "Optimal linear coding in white Gaussian channel with feedback," in *Proc. 2nd Japan-USSR Symp. Prob. Theory*, (Lecture Notes in Math, 330) pp. 120–123, Berlin: Springer Verlag, 1973.

The Average Number of Weighings to Locate a Counterfeit Coin

D. G. MEAD

***Abstract*—A solution is obtained to the problem of finding the minimum of the average number of weighings, using a balance, needed to locate one light coin from among n coins of which $n-1$ are genuine and of the same weight. Optimal strategies are determined, and the anomaly that it may be better to work with $n+1$ coins rather than n is examined and explained.**

The problem of minimizing the maximum number of weighings required, using a balance, to find one off-weight counterfeit coin (which we assume is lighter) from among n genuine coins of equal weight has been solved several times (e.g., [4] and [5]) and has also appeared in several introductory texts on information theory ([2, pp. 349–50], [3, p. 517]). Other problems of this type have appeared recently ([1]). However, no one appears to have considered the problem of minimizing the average number of weighings required, using a balance, to find the one counterfeit light coin from among n coins, $n-1$ of which are genuine coins of equal weight. The solution to the latter problem has some surprising consequences. For example, letting $f(n)$ be this minimum number, we shall see that $f(n)$ is not a monotonic function of n, and in particular $f(7)<f(6)$. This situation is not unusual and in fact occurs approximately one-fourth of the time. Also, as will be seen, given n, there are often many possible optimum strategies.

A strategy, at any stage, consists of placing a coins on each pan of the balance, and leaving b coins alone, where $2a+b$ equals the number of coins among which is the lighter coin. One might suspect that given, let us say, sixty-two coins, one of which is lighter, that the first step in a best strategy would be rather limited. In fact, one can minimize the average number of weighings by taking as the first step any $17 \leqslant a \leqslant 27$, with the exception of $a=20,24$. In fact, if x, $x+1$, $n-2x$, and $n-2(x+1)$ all lie between consecutive powers of three, then at least one of the strategies $a=x$ or $a=x+1$ is a best strategy.

Assume there are n coins, one of which is lighter than the rest, and let $f(n)$ be the minimum of the average number of weighings required to isolate the light coin using only a beam balance. We see that $f(n)$ satisfies

$$f(1)=0 \qquad f(2)=1 \qquad f(n)=\min_{2a+b=n}\left(1+\frac{2a}{n}f(a)+\frac{b}{n}f(b)\right).$$

Letting $f(n)=c(n)/n$, we note that $c(n)$ satisfies

$$c(1)=0 \qquad c(2)=2 \qquad c(n)=\min_{2a+b=n}(n+2c(a)+c(b)).$$

Manuscript received April 18, 1978.

The author is with the Department of Mathematics, University of California, Davis, CA, 95616.

We determine $c(n)$ and during the proof will verify the two general phenomena mentioned above.

Definition: If $n=3^k+4q+r<3^{k+1}$ where $0\leqslant q$,and $0\leqslant r<4$, let $c_1(n)=k\cdot n+6q+g(r)$ where $g(0)=0$, $g(1)=2$, $g(2)=3$, and $g(3)=6$. If $n=3^{k+1}-(4q+r)>3^k$ where $0\leqslant q$, $0\leqslant r<4$, let $c_2(n)=(k+1)n-2q-h(r)$, where $h(2)=1$, $h(r)=0$ if $r\neq 2$.

Theorem: $c(n)=c_1(n)=c_2(n)$.

The proof is broken into several parts. We first show that $c_1(n)=c_2(n)$ and then, in Lemma 3, that there is a best strategy with the first a and b lying between consecutive powers of three. This sufficiently limits the cases to be considered that we are able to carry out the calculations required for the proof.

Lemma 1: $c_1(n)=c_2(n)$.

Proof: Let $n=3^k+4q+r=3^{k+1}-(4t+s)$. Then since $3^{k+1}-3^k=[4(3^k-1)/2]+2$, $4q+r+4t+s=4[(3^k-1)/2]+2$. We must show that $kn+6q+g(r)=(k+1)n-(2t+h(s))$ or

$$6q+2t+g(r)+h(s)=n.$$

If $r=0,1,2$, then $t+q=(3^k-1)/2$, whence $6q+2t+g(r)+h(s)=2(t+q)+4q+g(r)+h(s)=3^k-1+4q+g(r)+h(s)=n$ since $g(r)+h(s)=r+1$ for $r=0,1,2$ $(s=2,1,0)$. For $r=3$, $s=3$, and $2(t+q)=3^k-3$. Thus $6q+2t+g(r)+h(s)=3^k-3+4q+6+0=3^k+4q+3=n$. This completes the proof that $c_1(n)=c_2(n)$. □

For fixed n, let $m(a)=2c_1(a)+c_1(b)$ where $2a+b=n$.

Lemma 2: i) If the minimum of $m(a)$ occurs with $b<3^k$ then the corresponding $a\leqslant 3^k+1$. ii) If the minimum of $m(a)$ occurs with $a<3^k$ then the corresponding $b\leqslant 3^k+3$.

Proof: a) If $a\geqslant 3^k$, then $c_1(a+2)-c_1(a)\geqslant 2k+2$. Similarly, if $b<3^k$, then $c_1(b)-c_1(b-4)\leqslant 4k+2$. Thus $m(a+2)-m(a)=2c_1(a+2)+c_1(b-4)-(2c_1(a)+c_1(b))\geqslant 2(2k+2)-4k-2=2$, or $m(a)<m(a+2)$. b) If $a<3^k$, $b\geqslant 3^k$, then $c_1(a)-c_1(a-2)\leqslant 2k+2$, $c_1(b+4)-c_1(b)\geqslant 4k+6$, and therefore $m(a-2)-m(a)\geqslant 4k+6-2(2k+2)=2$, or $m(a)<m(a-2)$. □

Lemma 3: There exists an l so that the minimum of $m(a)$ occurs with $3^{l-1}\leqslant a,b\leqslant 3^l$.

Proof: If the minimum occurs with $b<3^l$, then, by Lemma 2, $a\leqslant 3^l+1$. Assume the minimum occurs with $a=3^l+1$. Since for $3^{l-1}\leqslant x<3^l$, $c_1(x+1)-c_1(x)\leqslant l+2$, and $c_1(3^l+1)-c_1(3^l)=l+2$, it follows that $m(3^l+1)\geqslant m(3^l)$, or the minimum occurs with $a=3^l$.

Now we assume the minimum occurs with $a<3^l$ and $b\geqslant 3^l$. First note that $c_1(3^l+3)-c_1(3^l+1)=2l+4\geqslant 2[c_1(a+1)-c_1(a)]$. Hence $b\leqslant 3^l+2$. Now $c_1(3^l+2)-c_1(3^l)=2l+3$ and $c_1(3^l+1)-c_1(3^l-1)=2l+2$, while for $3^{l-1}\leqslant x<3^l$, $2(c_1(x+1)-c_1(x))\geqslant 2l+2$ only if $c_1(x+1)-c_1(x)=l+2$; this latter is true only if $x=3^l-4q$. However, in this case, $c_1(x+2)-c_1(x)=2l+1$, while $c_1(3^l+2)-c_1(3^l-2)=4l+4$ and $c_1(3^l+1)-c_1(3^l-3)=4l+2$. That is, $m(3^l+2)>m(3^l-2)$ and $m(3^l+1)\geqslant m(3^l-3)$. This completes the proof of the lemma. □

It is now easy to see that the minimum value of $m(a)$ occurs for one of two adjacent values of a. Note that if $3^l\leqslant x<3^{l+1}-2$ and $x-3^l\equiv y \pmod 4$ then

$$c_1(x+1)-c_1(x)=\begin{cases} l+2, & \text{if } y=0\\ l+1, & \text{if } y=1\\ l+3, & \text{if } y=2\\ l, & \text{if } y=3.\end{cases}$$

Hence

$$c_1(x+2)-c_1(x)=\begin{cases} 2l+3, & \text{if } y \text{ is even}\\ 2l+4, & \text{if } y=1\\ 2l+2, & \text{if } y=3.\end{cases}$$

But since $m(a)=2c_1(a)+c_1(b)$, it follows that as a increases, with $3^l\leqslant a$, $a+1$, $n-2a$, $n-2(a+1)\leqslant 3^{l+1}$, then $m(a+1)-m(a)$ runs through the sequence $1,-1,3,-3,1,-1,3,-3,\cdots$, or $0,0,2,-2,0,0,2,-2,\cdots$, or $2,-2,4,-4,2,-2,4,-4,\cdots$. From this we see that either $m(a)$ or $m(a+1)$ must be the

0018-9448/79/0900-0616$00.75 ©1979 IEEE