explicitly evaluable functions. For example, the M-ary error probability is expressed as a quadrature in Lindsey's equation (17),

$$P_E(M) = \frac{1}{2}\left[1 - \frac{\sqrt{2}}{\sqrt{\pi}}\int_0^\infty Q_M\left(h, \frac{x}{\sqrt{d}}\right)\exp\left(-\frac{x^2}{2}\right)dx\right]$$
$$= \frac{\sqrt{d}}{2\sqrt{\pi}}\frac{e^{-L}}{M!}\int_0^\infty e^{-(1+d)s}s^{M-1/2}\Phi_3(1, 1+M, s, sL)\,ds, \quad (5)$$

where, following Lindsey, $h^2/2$ has been replaced by L to simplify the notation.

From the series form of Φ_3, it is obvious that the integral gives an additional double series numerator parameter:

$$P_E(M) = \frac{\sqrt{d}}{2\sqrt{\pi}}\frac{e^{-L}}{M!}(1+d)^{-M-1/2}$$
$$\cdot\Phi_1\left(\tfrac{1}{2}+M, 1, 1+M, \frac{1}{1+d}, \frac{L}{1+d}\right). \quad (6)$$

A complete set of recursion relations for F_1 when one parameter at a time changes has been given by Le Vavasseur [8]. It is a simple matter to derive the necessary change for this two-parameter case but Le Vavasseur has included this as one of several examples, so that we have at once

$$\alpha(\gamma - \beta - \beta')F_1(\alpha+1, \beta, \beta', \gamma+1, x, y)$$
$$= \left[\alpha\gamma - \gamma(1-x)\frac{\partial}{\partial x} - \gamma(1-y)\frac{\partial}{\partial y}\right]$$
$$\cdot F_1(\alpha, \beta, \beta', \gamma, x, y), \quad (7)$$

whose confluent form is

$$\alpha\Phi_1(\alpha+1, \beta, \gamma+1, x, y) = \gamma\frac{\partial}{\partial y}\Phi_1(\alpha, \beta, \gamma, x, y). \quad (8)$$

Thus,

$$P_E(M) = \frac{\sqrt{d}}{2\sqrt{\pi}(1+d)^{3/2}}\frac{e^{-L}}{(\frac{3}{2})_{M-1}}$$
$$\cdot\frac{\partial^{M-1}}{(\partial L)^{M-1}}\Phi_1\left(\frac{3}{2}, 1, 2, \frac{1}{1+d}, \frac{L}{1+d}\right) \quad (9)$$
$$= e^{-L}\frac{\partial^{M-1}}{(\partial L)^{M-1}}[e^L P_E(1)] = \left(1 + \frac{\partial}{\partial L}\right)^{M-1}P_E(1),$$

which is equivalent to a result of Price [9], who has derived a number of expressions for these and related integrals.

Note that the derivation above is, thus far, much simpler and more straightforward than the admirably executed *tours de force* of previous derivations. However, the last step, viz., recognizing the form of the result, is automatically accomplished in the other derivations, and is much the harder part in the hypergeometric case. To obtain the reduction, we use operational relations [10] to get

$$\Phi_1(\alpha, 1, \gamma, x, y) = \sum_0^\infty \frac{(\alpha)_m(1)_m}{(\gamma)_m}\frac{x^m}{m!}{}_1F_1(\alpha+m; \gamma+m; y)$$
$$= \sum_0^\infty x^m\left(\frac{d}{dy}\right)^m {}_1F_1(\alpha; \gamma; y) \quad (10)$$
$$= \frac{1}{1 - x\dfrac{d}{dy}}\,{}_1F_1(\alpha; \gamma; y)$$
$$= e^{y/x}\int_y^\infty e^{-t/x}\,{}_1F_1(\alpha; \gamma; t)\,dt.$$

Furthermore [11],

$${}_1F_1(\tfrac{3}{2}; 2; 2t) = e^t[I_0(t) + I_1(t)]. \quad (11)$$

The integral with the special parameters of (11) has been previously recognized as a Q function [12]-[14] so that the reduction is essentially complete.

Acknowledgment

It is a pleasure to acknowledge my indebtedness to Dr. R. Price of the Sperry Rand Research Center, Sudbury, Mass., for a most valuable discussion on the subject of this note.

James A. Mullen
Research Division
Raytheon Company
Waltham, Mass.

References

[1] W. C. Lindsey, "Error probabilities for Rician fading multichan nel reception," *IEEE Trans. on Information Theory*, vol. IT-10, pp. 339-350, October 1964.
[2] J. I. Marcum, "A statistical theory of target detection by pulsed radar," *IEEE Trans. on Information Theory*, vol. 6, pp. 59-144, April 1960
[3] A. Erdélyi, W. Magnus, F. Oberhettinger, and F. Tricomi, *Higher Transcendental Functions*. New York: McGraw-Hill 1953, p. 155, sec. 2. 5. 4. vol. 1, and p. 87.
[4] *Ibid.* equation 9. 2. 1. (18), vol. 2, p. 136.
[5] *Ibid.* equation 5. 7. 1. (22), vol. 1, p. 225.
[6] *Ibid.* equation 5. 8. 2. (5), vol. 1, p. 231.
[7] *Ibid.* equation 5. 7. 1. (6), vol. 1, p. 224; for Φ_1, equation 5. 7. 1. (20), p. 225.
[8] P. Appell and J. Kampé de Fériet, *Fonctions hypergéométriques et hypersphériques*. Paris: Gauthier-Villars, 1926, p. 22; R. Le Vavasseur, *Sur le système d'équations aux dérivées partielles simultanées auxquelles satisfait la série hypergéométrique a deux variables F_1, Thèse* (Paris), no. 793, 1893; also, J. A. Mullen, "The differential recursion formulae for Appell's hypergeometric functions," to appear in *J. SIAM*, 1966.
[9] R. Price, "Some noncentral F-distributions expressed in closed form," *Biometrika*, vol. 51, pp. 107-122, equation (2.9), June 1964.
[10] I. I. Hirschman and D. V. Widder, *The Convolution Transform*. Princeton, N. J.: Princeton University Press, 1955, theorem 3.1, p. 6.
[11] Erdélyi et al. [3], equation 6. 9. 1. (10), vol. 1, p. 265; also equation 6.4. (12), vol. 1, p. 255.
[12] L. C. Maximon, "On the representation of indefinite integrals containing Bessel functions by simple Neumann series," *Proc. Am. Math. Soc.* vol. 7, pp. 1054-1062, December 1956.
[13] Price, [9], equation (5.2).
[14] Y. L. Luke, *Integrals of Bessel Functions*. New York: McGraw-Hill, 1962, pp. 287-288.

Run-Length Encodings

I. A Context for the Problem

Secret Agent 00111 is back at the Casino again, playing a game of chance, while the fate of mankind hangs in the balance. Each game consists of a sequence of favorable events (probability p), terminated by the first occurrence of an unfavorable event (probability $q = 1-p$). More specifically, the game is roulette, and the unfavorable event is the occurrence of 0, which has a probability of $q = 1/37$. No one seriously doubts that 00111 will come through again, but the Secret Service is quite concerned about communicating the blow-by-blow description back to Whitehall.

The bartender, who is a free-lance agent, has a binary channel available, but he charges a stiff fee for each bit sent. The problem perplexing the Service is how to encode the vicissitudes of the wheel so as to place the least strain on the Royal Exchequer. It is easily seen that, for the case $p = q = 1/2$, the best that can be done is to use 0 and 1 to represent the two possible outcomes. However, the case at hand involves $p \gg q$, for which the "direct coding" method is shockingly inefficient.

Finally, a junior code clerk who has been reading up on Information Theory, suggests encoding the *run lengths* between successive

Manuscript received May 6, 1965; revised November 9, 1965. This work was supported in part by the Jet Propulsion Laboratory under Contract 951076.

TABLE I
RUN-LENGTH DICTIONARIES FOR SMALL m

$m = 1$			$m = 2$			$m = 3$			$m = 4$		
n	$G(n)$	Codeword	n	$G(n)$	Codeword	n	$G(n)$	Codeword	n	$G(n)$	Codeword
0	1/2	0	0	0.293	00	0	0.206	00	0	0.151	000
1	1/4	10	1	0.207	01	1	0.164	010	1	0.128	001
2	1/8	110	2	0.116	100	2	0.130	011	2	0.109	010
3	1/16	1110	3	0.104	101	3	0.103	100	3	0.092	011
4	1/32	11110	4	0.073	1100	4	0.081	1010	4	0.078	1000
5	1/64	111110	5	0.051	1101	5	0.064	1011	5	0.066	1001
6	1/128	1111110	6	0.036	11100	6	0.051	1100	6	0.056	1010
7	1/256	11111110	7	0.025	11101	7	0.041	11010	7	0.048	1011
8	1/512	111111110	8	0.018	111100	8	0.032	11011	8	0.040	11000
9	1/1024	1111111110	9	0.013	111101	9	0.026	11100	9	0.034	11001
10	1/2048	11111111110	10	0.009	1111100	10	0.021	111010	10	0.029	11010

unfavorable events. In general, the probability of a run length of n is $p^n q$, for $n = 0, 1, 2, 3,...$, which is the familiar *geometric distribution.* (See Feller,[1] page 174.)

II. The Encoding Procedure

If the list of possible outcomes were finite, we could list them with their probabilities, and apply Huffman coding[2] (as done by Abramson,[3] page 77 et seq.). However, with an infinite list, it is clear that we cannot start at the bottom and work our way up. Fortunately, the fact that the probabilities follow a distribution law furnishes a short cut, as follows.

Let $m = -\log 2/\log p$. (That is, $p^m = 1/2$.) The results will be most readily applicable for those p such that m is an integer (viz., $p = 0.5, p = 0.707..., p = 0.794..., p = 0.849..., p = 0.873...$, etc.). The resulting coding scheme is especially simple when m is a power of 2, but *any* integer m is a favorable case.

If $p^m = 1/2$, then a run of length $n + m$ is only half as likely as a run of length n. (The respective probabilities are $p^{m+n} q = \frac{1}{2} p^n q$ and $p^n q$.) Thus, we would expect the codeword for run-length $n + m$ to be one bit longer than the codeword for run-length n. This argument, although nonrigorous, leads to the correct conclusion that there should be m codewords of each possible wordlength, except for the shortest wordlengths, which are not used at all if $m > 1$, and possibly one transitional wordlength which is used fewer than m times. Knowing this answer, there is a rigorous proof by mathematical induction. The dictionaries for the first several values of m are as shown in Table I, where $G(n)$ is used to designate $p^n q$.

In general, let k be the smallest positive integer such that $2^k \geqq 2m$. Then the corresponding code dictionary contains exactly m words of every word length $\geqq k$, as well as $2^{k-1} - m$ words of length $k - 1$. (The simplification which occurs for m a power of 2 is that the collection of words of length $k - 1$ is empty.) This result is obtained by seeing how much "signal space" is used up by having m words of every length $\geqq k$. This consumes

$$\frac{m}{2^k} + \frac{m}{2^{k+1}} + \frac{m}{2^{k+2}} + \cdots = \frac{m}{2^{k-1}},$$

leaving $1 - m/2^{k-1} = (2^{k-1} - m)/2^{k-1}$ unused, which means that $2^{k-1} - m$ words of length $k-1$ may be adjoined.

III. Further Examples

We will consider the cases $m = 14$ and $m = 16$, to illustrate what happens when m is not a power of 2 and when m is a power of 2, respectively. The dictionaries in these two cases are shown in Table II. In the case $m = 14$, we find $k = 5$, and $2^{k-1} - m = 2$, so that there are two codewords of length 4, followed by fourteen codewords of lengths 5, 6, 7, etc. On the other hand, since $m = 16$ is a power of 2, the corresponding dictionary contains exactly 16 words of every wordlength starting with length 5.

In a practical situation, if $m = -\log 2/\log p$ is not an integer, then the best dictionary will oscillate between $[m]$ words of a given length and $[m] + 1$ words of another length. (Here $[m]$ denotes the greatest integer $\leqq m$.) For large m, however, there is very little penalty for picking the *nearest* integer when designing the code. Very often, the underlying probabilities are not known accurately enough to justify picking a non-integral value of m. (For example, saying $p = 0.95$ on the basis of statistical evidence may involve as large a round-off error as saying $m = 14$.) For Agent 00111, the approximation $m = 25$ corresponds closely to $q = 1/37$.

TABLE II
RUN-LENGTH DICTIONARIES FOR $m = 14$ AND $m = 16$

$m = 14$				$m = 16$			
n	Codeword	n	Codeword	n	Codeword	n	Codeword
0	0000	24	101100	0	00000	24	101000
1	0001	25	101101	1	00001	25	101001
		26	101110	2	00010	26	101010
2	00100	27	101111	3	00011	27	101011
3	00101	28	110000	4	00100	28	101100
4	00110	29	110001	5	00101	29	101101
5	00111			6	00110	30	101110
6	01000	30	1100100	7	00111	31	101111
7	01001	31	1100101	8	01000		
8	01010	32	1100110	9	01001	32	1100000
9	01011	33	1100111	10	01010	33	1100001
10	01100	34	1101000	11	01011	34	1100010
11	01101	35	1101001	12	01100	35	1100011
12	01110	36	1101010	13	01101	36	1100100
13	01111	37	1101011	14	01110	37	1100101
14	10000	38	1101100	15	01111	38	1100110
15	10001	39	1101101			39	1100111
		40	1101110	16	100000	40	1101000
16	100100	41	1101111	17	100001	41	1101001
17	100101	42	1110000	18	100010	42	1101010
18	100110	43	1110001	19	100011	43	1101011
19	100111			20	100100	44	1101100
20	101000	44	11100100	21	100101	45	1101101
21	101001	45	11100101	22	100110	46	1101110
22	101010	46	11100110	23	100111	47	1101111
23	101011	47	11100111				

IV. Decoding

The dictionaries in Table II exhibit striking patterns which suggest that a rather simple decoding procedure might be employed. For the case $m = 16$, the following rule for decoding is adequate.

Start at the beginning (left end) of the word, and count the number of 1's preceding the first 0. Let this number be $A \geqq 0$. Then the word consists of $A + 5$ bits. Let the last 5 bits be regarded as the ordinary binary representation of the integer R, $0 \leqq R \leqq 15$. Then the correct decoding of the word is $16A + R$. This simple decoding reveals an equally simple method of *encoding.* To encode the number N, we divide N by 16 to get $N = 16A + R$, and write A 1's followed by the 5-bit binary representation of R.

The case $m = 14$ is only slightly more complicated. Suppose a word starts in A 1's, and the next three bits are *not all 0's.* Then we consider the word to consist of $A + 5$ bits altogether. Let the last 5 bits be the binary representation of the integer R. Then the correct decoding of the codeword is $14A + R - 2$. On the other hand, if the initial A 1's are followed by three or more 0's, we regard the codeword as consisting of a total of $A + 4$ bits. Letting the last 4 bits be the binary representation of an integer R', the correct decoding in this case is $14A + R'$. This procedure also can be inverted to describe direct encoding from ordinary numbers to codewords.

[1] W. Feller, *An Introduction to Probability Theory and Its Applications*, vol. 1. New York: Wiley, 1950.
[2] D. Huffman, "A method for the construction of minimum redundancy codes," *Proc. IRE*, vol. 40, pp. 1098–1101, September 1952.
[3] N. Abramson, *Information Theory and Coding.* New York: McGraw-Hill, 1963.

V. Implementation

The Senior Cryptographer observes that although run length coding is a big improvement over no coding at all, it is less than 100 percent efficient for the mission at hand. He has heard that a method invented at M.I.T. is 100 percent efficient. However, a hasty briefing on this method convinces Operations that it is unimplementable, because it requires infinite computing capability. The run-length system is employed after all. As it turns out, however, Agent 00111 has bribed the croupier, and the "Unfavorable Case" occurs only half as often as expected. Fortunately, the coding procedure is such that the cost of communicating has also decreased as a result!

It is appropriate to mention that there really is a method, invented by Elias and Shannon (see Abramson,[3] page 61), which is 100 percent efficient for communicating events from a p: q distribution. Moreover, the assertion that "infinite computing capability" is required is a gross overstatement. Nevertheless, British Intelligence quite possibly made the correct practical decision. We shall leave it to the reader to judge.

VI. Perspective

The literature in statistical communication theory generally contains a significant shift in viewpoint between the discrete and the continuous case. In the latter context, a particular distribution is assumed almost from the outset, and most of the theorems refer to such things as the "white Gaussian noisy channel," or other equally specific assumptions. For the discrete case, on the other hand, the results are rarely evaluated in terms of specific distributions. The present remarks are intended as a step in this direction, viz., the explicit form which Huffman coding assumes when applied to the geometric distribution. It would also be appropriate to have explicit answers for the binomial distribution, the Poisson distribution, etc.

Solomon W. Golomb
Dept. of Elec. Engrg.
University of Southern California
Los Angeles, Calif.

A Remark Concerning the Existence of Binary Quasi-Perfect Codes

It is an easy exercise to show that if there exist single error-correcting quasi-perfect (*SEC QP*) codes with m check bits for block lengths n_1 and n_2 ($n_1 < n_2$), then there exist *SEC QP* codes with m check bits for all block lengths n with $n_1 < n < n_2$. It would be useful to know whether this statement generalizes to t error-correcting codes. (See Peterson[1] for definitions.)

In the course of using a tree-search technique for finding quasi-perfect codes on a digital computer (see Wagner[2]), the writer noticed that for $t = 2$ some quasi-perfect codes were never found which the above statement, if true, indicated existed. Since the computer search was by no means exhaustive, a counter-example was not found. Recently, an exhaustive search along the lines of Wagner[2] has revealed that a double error-correcting quasi-perfect (16, 8) code does not exist. Since *DEC QP* (14, 6), (15, 7), and (17, 9) codes exist, this provides a counter-example to the statement for $t = 2$.

Terry J. Wagner
Dept. of Elec. Engrg.
University of Texas
Austin, Tex.

Manuscript received September 27, 1965. This work was supported by the National Science Foundation under Grant GP 3012.

[1] W. W. Peterson, *Error Correcting Codes*. Cambridge, Mass.: M.I.T. Press, 1961.

[2] T. J. Wagner, "A search technique for quasi-perfect codes," *Information and Control*, vol. 9, pp. 94–99, February 1966.

Analysis of Weight Distribution in Binary Cyclic Codes

Bose-Chaudhuri codes constitute the presently best-known class of binary codes for correction of independent errors. The most interesting property of these codes is that a lower bound for minimum distance can be given by an a priori algebraic argument. It can, however, be shown in a number of cases that either these codes actually correct more errors than one is able to prove, or that there exists cyclic codes of the same size that have larger minimum distance. It seems thus interesting to dispose of easily mechanized methods of analysis for such codes. In a recent paper, MacWilliams[1] outlines a method of attack based on an extensive analysis of their algebraic structure. Our own research led us to similar methods and to some additional results briefly discussed herein.

Firstly, the process of finding *cycle representatives* in a minimal ideal[2] is not as laborious as stated,[3] since it can be easily mechanized utilizing the isomorphism between a minimal ideal M generated by

$$g(x) = (x^n - 1)/h(x) \tag{1}$$

and the Galois Field $GF(2^k)$ modulo the irreducible polynomial $h(x)$ of degree k. Let n' be the exponent to which $h(x)$ belongs; then all vectors in M have the same cycle length n' and there exist

$$m' = (2^k - 1)/n' \tag{2}$$

cycle representatives. As shown by Nili,[4] the elements

$$g(x);\ \alpha(x)\cdot g(x);\ \alpha^2(x)g(x);\ \cdots\ \alpha^{m'-1}(x)\cdot g(x) \tag{3}$$

where $\alpha(x)$ is any primitive root in the Galois Field $GF(2^k)$, are the cycle representatives of M. Instead of $g(x)$, the primitive idempotent[5] $\varepsilon(x)$ may be used to generate the ideal M, and the cycle representatives become

$$\varepsilon(x);\ \alpha(x)\cdot\varepsilon(x);\ \alpha^2(x)\cdot\varepsilon(x);\ \cdots\ \alpha^{m'-1}(x)\cdot\varepsilon(x). \tag{4}$$

It is no longer necessary to compute the weights of all elements in (4), since, for example, the vectors

$$v(x) = \alpha^i(x)\cdot\varepsilon(x)$$

and

$$v^2(x) = \alpha^{2i}(x)\cdot\varepsilon(x)$$

have the same weight. The sequence (4) can be divided into automorphism classes by squaring; the exponents of $\alpha(x)$ in such a class are in one cycle[6] $\sum_2(m')$ and there exists a one-to-one correspondence between these cycles and the irreducible factors of $x^{m'}-1$ over the binary field. Only one element of each automorphism class need be considered in order to have a compact weight-representation of the ideal M. The process of finding such representatives can easily be mechanized on a computer, and some codes have been studied in this way. The following weight distribution of the (41, 21) cyclic code has been computed in ten seconds on a medium capacity computer (add time ten microsencond) in Table I. Table II gives the minimum distance (probably new) of several cyclic codes.

The method can be generalized to every ideal, since[7] any ideal is the direct sum[8] of the minimal ideals contained in it. Some refinements of the method are being studied for further publication.

Manuscript received June 1, 1965; revised October 19, 1965.

[1] J. MacWilliams, "The structure and properties of binary cyclic alphabets," *Bell Sys. Tech. J.*, vol. 44, pp. 303–333, February 1965.

[2] A set of vectors obtained from each other by shifting cyclically the components is called a cycle. The cycle length is the number of distinct vectors in such a cycle. A set of *cycle representatives* is obtained by choosing one vector out of each cycle.

[3] MacWilliams, [1] page 315.

[4] H. Nili, "Matrixschaltungen zur Codierung und Decodierung von Gruppen-Code," *Arch. eleck. Übertragung*, vol. 18, pp. 555–565, September 1964.

[5] MacWilliam,[1] lemma 2.6, page 322.

[6] *Ibid.*, page 306.

[7] *Ibid.*, lemma 2.12 (*iii*).

[8] Rather than *union*, as it is called by MacWilliams.[1]