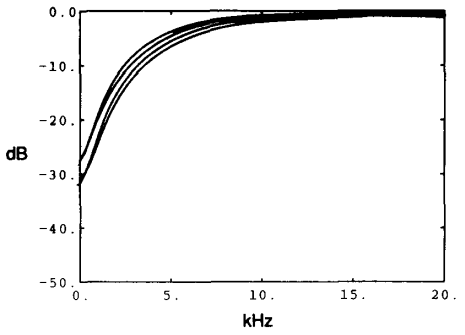

Fig. 5. Simulated PSD's of coded 256-QAM signals at $f = 0$. Symbol rate is 2 Mbaud. The OF01 with 0.5 percent, the OF00 with 1 percent, the FJ01 with 2 percent, and the FJ00 with 4 percent redundancy are used for coding.

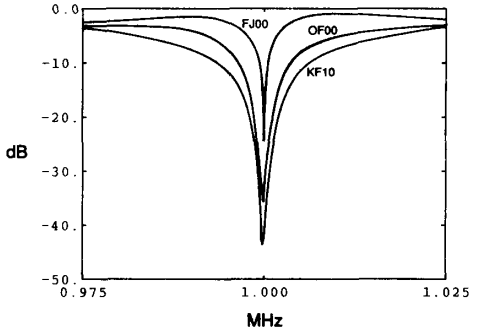

Fig. 6. Simulated PSD's of coded 256-QAM signals at the Nyquist frequency. Redundancy in all codes is 1 percent. Symbols rate is 2 Mbaud. The KF10, OF00, and FJ00 codes are compared.

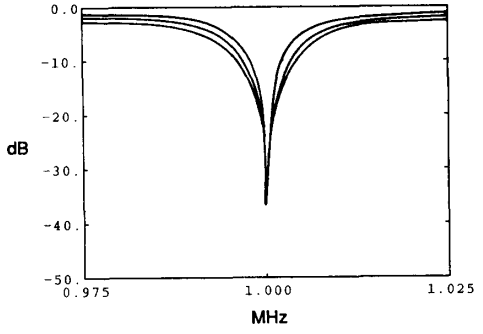

Fig. 7. Simulated PSD's of coded 256-QAM signals at the Nyquist frequency. Symbols rate is 2 Mbaud. The KF10 with 0.5 percent, the OF00 with 1 percent, and the FJ00 with 4 percent redundancy are used for coding.

References

[1] Y. Daido *et al.*, "Multilevel QAM modulation techniques for digital microwave radios," *IEEE J. Select. Areas in Commun.*, vol. SAC-5, pp. 336-341, Apr. 1987.

[2] K. Feher, "1024-QAM and 256-QAM coded modems for microwave and cable system applications, *IEEE J. Select. Areas Commun.*, vol. SAC-5, pp. 357-368, Apr. 1987.

[3] A. J. Bateman and J. P. McGeehan, "Phased-locked transparent tone-in-band (TTIB): A new spectrum configuration particularly suited to the transmission of data over SSB mobile radio networks," *IEEE Trans. Commun.*, vol. COM-32, pp. 81-87, Jan. 1984.

[4] F. Davarian, "Mobile digital communications via tone calibration," *IEEE Trans. Vehic. Technol.*, vol. VT-36, pp. 55-62, May 1987.

[5] M. K. Simon, "Dual-pilot tone calibration technique," *IEEE Trans. Vehic. Technol.*, vol. VT-35, pp. 63-70, May 1986.

[6] H. Kaneko and A. Sawai, "Feedback balanced code for multilevel PCM transmission," *IEEE Trans. Commun.*, vol. COM-17, pp. 554-653, Oct. 1969.

[7] S. Hagiwara, N. Sata, and A. Tokimasa, "1.544 Mbits/sec PCM-FDM converters over coaxial and microwave systems," *Fujitsu Sci. Tech. J.*, pp. 1-26, Sept. 1976.

[8] J. Orton and K. Feher, "A new channel coding algorithm for in-band spectral suppression in PAM and QAM systems," in *Rec. Int. Conf. Commun.*, Philadephia, PA, pp. 21.5.1-21.5.5.

[9] D. Y. Kim and J.-K. Kim, "A condition for stable minimum-bandwidth line codes," *IEEE Trans. Commun.*, vol. COM-33, pp. 152-157, Feb. 1985.

[10] E. Gorog, "Redundant alphabets with desirable frequency spectrum properties," *IBM J. Res. Develop.* vol. 12, pp. 234-240, May 1968.

[11] G. L. Pierobon, "Codes for zero spectral density at zero frequency," *IEEE Trans. Inform. Theory*, vol., IT-30, pp. 435-439, Mar. 1984.

[12] D. Y. Kim and K. Feher, "New carrier and symbol synchronization technique for digital mobile systems," in *Rec. IEEE Vehic. Technol. Conf.*, Philadephia, PA, June 1988, pp. 371-376.

[13] C. M. Monti and G. L. Pierobon, "Block codes for linear timing recovery in data transmission systems," *IEEE Trans. Commun.*, vol. COM-33, pp. 527-534, June 1985.

[14] P. S. K. Leung and K. Feher, "Block-inversion-coded QAM systems," *IEEE Trans. Commun.* July 1988.

Error Detecting Capabilities of the Shortened Hamming Codes Adopted for Error Detection in IEEE Standard 802.3

TORU FUJIWARA, TADAO KASAMI, AND SHU LIN

***Abstract*—In this paper, we investigate the error detecting capabilities of the shortened Hamming codes adopted for error detection in IEEE Standard 802.3. These codes are also used for error detection in the data link layer of the Ethernet, a local area network. We compute the weight distributions for various code lengths. From the results, we show the probability of undetectable error and that of detectable error for a binary symmetric channel with bit-error rate $10^{-5} \leq \epsilon \leq 1/2$. We also find the minimum distance of the shortened code of length n for $33 \leq n \leq 12144$ and the double-burst detecting capabilities.**

I. Introduction

In this paper, we investigate the error detecting capabilities of the shortened Hamming codes adopted for error detection in IEEE Standard 802.3 [1]. These codes are also used for error

Paper approved by the Editor for Coding Theory and Applications of the IEEE Communications Society. Manuscript received May 24, 1988; revised July 25, 1988. This work was supported in part by NSF Grant DCI-8418248 and NASA Grant NAG 5-931. This paper was presented in part at the 1986 IEEE International Symposium and Information Theory, Ann Arbor, MI, October 1986.

T. Fujiwara and T. Kasami are with the Faculty of Engineering Science, Osaka University, Toyonaka, Osaka, 560 Japan.

S. Lin is with the Department of Electrical Engineering, University of Hawaii at Manoa, Honolulu, HI 96822.

IEEE Log Number 8929601.

TABLE I
THE NUMBER OF THE CODEWORDS OF WEIGHT i FOR C_n

	n = 512	n = 1024	n = 2048	n = 4096	n = 8192	n = 12144
i=3	0	0	0	0	0	0
i=4	0	0	0	1168	47983	223059
i=5	212	3334	73464	2218860	71059586	510671733
i=6	6665	361454	23644314	1523208762	97571278763	1035951197006
i=7	427394	53429054	6908644559	888971303068	1.1408371219E+14	1.7963513870E+15
i=8	25836213	6793480175	1762848701492	4.5438944144E+14	1.1672244885E+17	2.7252863955E+18
i=9	1445275850	766784326346	3.9957866584E+14	2.0639394631E+17	1.0613959209E+20	3.6748972244E+21
i=10	72705347098	77827557042064	8.1474029231E+16	8.4353205238E+19	8.6854028852E+22	4.4594877862E+24
i=11	3318012052055	7.1742663440E+15	1.5094917001E+19	3.1333381609E+22	6.4603605823E+25	6.4603605823E+25
i=12	1.3852737738E+14	6.0562757186E+17	2.5623621702E+21	1.0666405322E+25	4.4043508270E+28	4.9737417959E+30
i=13	5.3279748701E+15	4.7145777286E+19	4.0130533669E+23	3.3508922567E+27	2.7713530588E+31	4.6416488821E+33
i=14	1.8990424707E+17	3.4045986309E+21	5.8332597153E+25	9.7726379171E+29	1.6190640477E+34	4.0219887564E+36
i=15	6.3048211511E+18	2.2924297453E+23	7.9099001739E+27	2.6594605318E+32	8.8271371882E+36	3.2524482410E+39
i=16	1.9584350687E+20	1.4456635081E+25	1.0050516909E+30	6.7832865190E+34	4.5112187992E+39	2.4655590447E+42
i=17	5.7140223158E+21	8.5719342130E+26	1.2013323740E+32	1.6279887646E+37	2.1696308766E+42	1.7589588291E+45
i=18	1.5713561369E+23	4.7955209736E+28	1.3555033620E+34	3.6892034282E+39	9.8537402313E+44	1.1850496511E+48
i=19	4.0855259659E+24	2.5391021576E+30	1.4482483289E+36	7.9181955684E+41	4.2391827711E+47	7.5631116155E+50
i=20	1.0070821481E+26	1.2758988342E+32	1.4692479296E+38	1.6141241666E+44	1.7323420394E+50	4.5851364169E+53
i=21	2.3594496042E+27	6.1000115692E+33	1.4188737149E+40	3.1329381444E+46	6.7412853077E+52	2.6471520913E+56
i=22	5.2658625257E+28	2.7810507290E+35	1.3072986455E+42	5.8030558810E+48	2.5037746477E+55	1.4587011274E+59
i=23	1.1218576685E+30	1.2115707959E+37	1.1515595895E+44	1.0278978113E+51	8.8938429876E+57	7.6879891594E+61
i=24	2.2857849996E+31	5.0532598611E+38	9.7162840363E+45	1.7444282439E+53	3.0272418069E+60	3.8827548584E+64
i=25	4.4618523192E+32	2.0213039444E+40	7.8663035558E+47	2.8413247236E+55	9.8906044315E+62	1.8823595553E+67
i=26	8.3573926133E+33	7.7664716942E+41	6.1205892667E+49	4.4488588269E+57	3.1067910151E+65	8.7739674812E+69
i=27	1.5043306704E+35	2.8707180559E+43	4.5836412953E+51	6.7062427502E+59	9.3963168256E+67	3.9378865903E+72
i=28	2.6057156255E+36	1.0221806792E+45	3.3084068063E+53	9.7456077680E+61	2.7400331029E+70	1.7041204219E+75
i=29	4.3488495267E+37	3.5106619188E+46	2.3044764651E+55	1.3670735310E+64	7.7136656042E+72	7.1196975973E+77
i=30	7.0016477380E+38	1.1643695364E+48	1.5509126610E+57	1.8532960169E+66	2.0988884109E+75	2.8751712131E+80

detection in the data link layer of the Ethernet [2], a local area network. The generator polynomial of these codes is

$$g(X)=X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^8+X^7+X^5+X^4+X^2+X+1 \quad (1)$$

which is primitive polynomial of degree 32.

Let C_n be a shortened code of length n. The code length n should be a multiple of 8 with $512 \le n \le 12144$ for the frame format of MAC (Media Access Control) sublayer of the data link layer in IEEE Standard 802.3 [1], as well as that of the data link layer for the Ethernet [2]. In Section II, we show the weight distributions of codes C_n for $n = 2^p$ with $9 \le p \le 13$ and $n = 12\ 144$. Note that 2^9 and 12 144 are the shortest and longest code lengths of the IEEE Standard, respectively. We also show the probability of undetectable error and that of detectable error for a binary symmetric channel with bit-error rate $10^{-5} \le \epsilon \le 1/2$ for these code lengths. In Section III, we list the minimum distances of codes C_n for $33 \le n \le 12\ 144$. In Section IV, for an integer b with $9 \le b \le 16$, we compute the maximum code length n_b such that C_{n_b} has the capability of detecting any double-burst error pattern which consists of two burst errors of length b or less.

II. Weight Distributions, Probability of Undetectable Error, and That of Detectable Error

For integers n and i with $33 \le n < 2^{32}$ and $0 \le i \le n$, let $A_{n,i}$ and $B_{n,i}$ be the number of codewords of weight i in C_n and that in the dual code of C_n, respectively. We have computed $\{B_{n,i}: 0 \le i \le n\}$ for $n = 2^p$ with $9 \le p \le 13$ and $n = 12\ 144$ by using method II in [3]. It takes about 1800 s to compute $\{B_{n,i}: 0 \le i \le n\}$ for each n with an NEC High Speed Fortran Processor (37 MIPS). We also computed $\{A_{n,i}: 0 \le i \le n\}$ for these code lengths by using MacWilliams' identity. In Table I, we show $\{A_{n,i}: 3 \le i \le 30\}$ for $n = 2^p$ with $9 \le p \le 13$ and $n = 12144$.

Let $P_e(C_n, \epsilon)$ denote the probability of an undetected error when code C_n is used for error detection on a binary symmetric channel with bit-error rate ϵ. $P_e(C_n, \epsilon)$ can be expressed in the following two forms:

$$P_e(C_n, \epsilon) = \sum_{i=1}^{n} A_{n,i}\epsilon^i(1-\epsilon)^{n-i}$$

$$= 2^{-32}\sum_{i=0}^{n} B_{n,i}(1-2\epsilon)^i - (1-\epsilon)^n. \quad (2)$$

The probability that an error is detected, $P_d(C_n, \epsilon)$, is

$$P_d(C_n, \epsilon) = 1 - P_e(C_n, \epsilon) - (1-\epsilon)^n. \quad (3)$$

In Figs. 1 and 2, we show $P_e(C_n, \epsilon)$ and $P_d(C_n, \epsilon)$, respectively, with bit-error rate $10^{-5} \le \epsilon \le 1/2$ for $n = 2^p$ with $9 \le p \le 13$ and $n = 12144$.

III. Minimum Distances of the Codes

It is well known that the minimum distance, denoted d_n, of C_n satisfies that

$$d_{2^{32}-1} = 3 \quad (4)$$

and $d_n \ge 3$ for $33 \le n < 2^{32} - 1$. But, in general, the exact minimum distance for a shortened Hamming code is unknown. In this section, we show d_n for $33 \le n \le 12144$.

Since $d_n \ge d_{n'}$ if $n < n'$, we see from Table I that

$$d_n = 5, \quad \text{for } 512 \le n \le 2048 \quad (5)$$

$$d_n = 4, \quad \text{for } 4096 \le n \le 12144. \quad (6)$$

By generating all the codewords of C_n for $33 \le n \le 54$, we found that

$$d_n = 15, \quad \text{for } 33 \le n \le 42 \quad (7)$$

$$d_n = 12, \quad \text{for } 43 \le n \le 44 \quad (8)$$

$$d_n = 11, \quad \text{for } 45 \le n \le 53 \quad (9)$$

$$d_n = 10, \quad \text{for } n = 54. \quad (10)$$

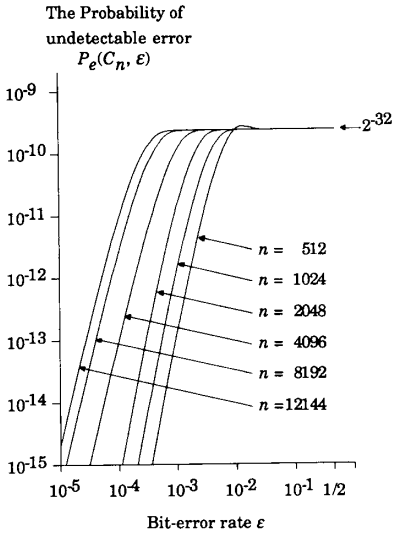

Fig. 1. The probability that a received vector contains an undetectable error pattern, denoted $P_e(C_n, \epsilon)$, for a binary symmetric channel with bit-error rate ϵ.

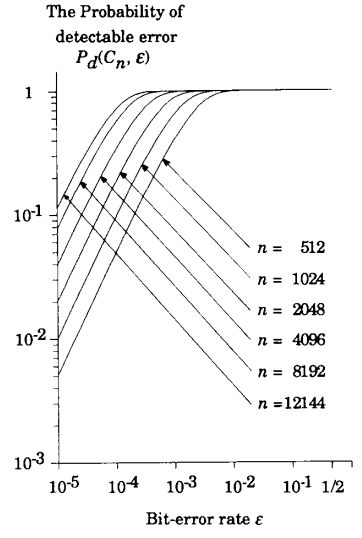

Fig. 2. The probability that a received vector contains a detectable error pattern, denoted $P_d(C_n, \epsilon)$, for a binary symmetric channel with bit-error rate ϵ.

The remaining problem is to determine d_n for $55 \le n < 512$ and $2048 < n < 4096$. It follows from (5), (6), and (10) that

$$4 \le d_n \le 5, \qquad \text{for } 2048 < n < 4096 \tag{11}$$

$$5 \le d_n \le 10, \qquad \text{for } 55 \le n < 512. \tag{12}$$

Let $n(d)$ be the minimum code length of C_n's which have the minimum distance d or less. For each d with $4 \le d \le 9$, we compute $n(d)$ by the method shown in the Appendix. In Table II, we show d_n for $33 \le n \le 12\,144$. It takes 77 s to compute $n(d)$ for $4 \le d \le 9$.

TABLE II
MINIMUM DISTANCE OF C_n

code length n	minimum distance d_n
$3007 \le n \le 12144$	4
$301 \le n \le 3006$	5
$204 \le n \le 300$	6
$124 \le n \le 203$	7
$90 \le n \le 123$	8
$67 \le n \le 89$	9
$54 \le n \le 66$	10
$45 \le n \le 53$	11
$43 \le n \le 44$	12
$33 \le n \le 42$	15

IV. Double-Burst Error-Detecting Capability

When a shortened cyclic code with generator polynomial of degree m is used for error detection, it is known [4] that

1) any single-burst error pattern of length m or less can be detected, and

2) the ratio of undetectable single-burst error patterns of length b with $b > m$ to all the burst error patterns of length b is

a) $1/2^{m-1}$, if $b = m+1$

b) $1/2^m$, otherwise.

In this section, we consider double-burst error patterns. A double b-burst error is an error pattern consisting of two single-burst error patterns of length b or less. Any double b-burst is detectable if and only if any single-burst error of length b or less can be corrected. For a positive integer b, let n_b be the maximum code length such that C_{n_b} has the capability of correcting any single-burst error of length b or less. We compute n_b for $9 \le b \le 16$ by using the algorithm in [5]. The results are shown in Table III.

Appendix

A Method for Computing $n(d)$

From (6) and (10), we have that

$$55 \le n(d) \le 4096, \qquad \text{for } 4 \le d \le 9.$$

Let h be a predesigned integer. For $4 \le d \le 7$, we chose $h = 2$, and for $8 \le d \le 9$, we chose $h = 3$. For integers n, d, and h, define the following sets of polynomials:

$$S_1(n, d, h) = \{1 + X^{j_1} + X^{j_2} + \cdots + X^{j_{d-h-2}} + X^{n-1}: 0 < j_1 < j_2 < \cdots < j_{d-h-2} < n\},$$

$$S_2(n, h) = \{X^{i_1} + X^{i_2} + \cdots + X^{i_h}: 0 < i_1 < i_2 < \cdots < i_h < n-1\}.$$

Then $n(d)$ is the smallest n such that there is a polynomial pair $n_1(X)$ in $S_1(n, d, h)$ and $p_2(X)$ in $S_2(n, h)$ which satisfy

$$p_1(X) \bmod g(X) = p_2(X) \bmod g(X)$$

and the number of nonzero coefficients of polynomial $p_1(X) + p_2(X)$ is d. Hence, for each polynomial $p_1(X)$ in $S_1(n, d, h)$ with $n \ge 55$, by checking whether or not there is such a polynomial $p_2(X)$ in $S_2(n, h)$, we can find $n(d)$. This can be

TABLE III
DOUBLE-BURST ERROR DETECTING CAPABILITY OF C_n

code length n	burst error length b^*
$11994 \le n \le 13000$	9
$5681 \le n \le 11993$	10
$1730 \le n \le 5680$	11
$731 \le n \le 1729$	12
$39 \le n \le 730$	13
$33 \le n \le 38$	16

* C_n has the capability of detecting any double-burst error which consists of two single-burst errors of length b or less.

done easily by using a hashing table by which for a given polynomial $m(X)$ of degree less than 32, we can check whether or not there is a polynomial $p_2(X)$ in the set $S_2(n, h)$ such that

$$p_2(X) \bmod g(X) = m(X)$$

and find the coefficients of $p_2(X)$ if they exist.

Since the numbers of polynomials in the sets $\cup_{55 \le n \le n(d)} S_1(n, d, h)$ and $\cup_{55 \le n \le n(d)} S_2(n, h)$ are $O(\{n(d)\}^{d-h-1})$ and $O(\{n(d)\}^h)$, respectively, the order of computing time is $O(\min\{\{n(d)\}^{d-h-1}, \{n(d)\}^h\})$ where $\{n(d)\}^h$ is the computing time for constructing the hashing table. The space complexity of this method is $O(\{n(d)\}^h)$ which is the size of the hashing table.

REFERENCES

[1] ANSI/IEEE Standard for Local Area Networks, "Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications," 1984.

[2] DEC, Intel, and Xerox, "The Ethernet: A local area network data link layer and physical layer specifications," version 1.0, 1980.

[3] T. Fujiwara, T. Kasami, A Kitai, and S. Lin, "On the undetected error probability for shortened Hamming codes," *IEEE Trans. Commun.*, vol. COM-33, pp. 570–574, June 1985.

[4] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, 2nd ed. Cambridge, MA: M.I.T. Press, 1972.

[5] T. Kasami, "Optimum shortened cyclic codes for burst-error correction," *IEEE Trans. Inform. Theory*, vol. IT-9, no. 2, pp. 105–109, 1963.

A Simple Series for Personal Computer Computation of the Error Function $Q(\cdot)$

NORMAN C. BEAULIEU

Abstract—**A simple series for computation of the error function $Q(\cdot)$ is derived. It is well suited for implementation on a personal computer, having six or more significant figure accuracy over a wide range of argument and requiring few lines of code to program. Its advantage over other series is its rapid convergence over a wide range of argument.**

Paper approved by the Editor for Fading, Dispersive, and Multipath Channels of the IEEE Communications Society. Manuscript received August 18, 1988. This work was supported in part by NSERC Grant A-3986 and Queen's University Research Initiation funding.

The author is with the Department of Electrical Engineering, Queen's University, Kingston, Ont., Canada K7L 3N6.

IEEE Log Number 8929602.

I. INTRODUCTION

Noise in digital communication systems is frequently assumed to possess an amplitude probability density function that is Gaussian. Consequently, the error probability of many systems is expressed in terms of the error function $Q(\cdot)$ where

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-t^2/2}\, dt \tag{1}$$

is the area under the tail of the unit Gaussian density function.

In this correspondence, we derive a simple series approximation to $Q(\cdot)$. The aim is to obtain an algorithm which is simple, requiring only a few lines of code to implement, yet accurate over a wide range of argument. These criteria are motivated by the widespread use of personal computers (PC's) to solve communication problems. A simple algorithm that can be coded in a few lines is quick to program, and hence transportable. At the same time, one wants sufficient accuracy to ensure graphical precision for those cases where the PC is used to generate a curve on a plotter. For full-scale plots (8–10 inch height), three significant figure accuracy is required if $Q(\cdot)$ itself is plotted directly. Note that in cases where $Q(\cdot)$ enters an analysis at an intermediate stage, the inherent loss of accuracy of numerical computation may require that $Q(\cdot)$ be accurate to five or six significant figures to ensure that there is three significant figure accuracy in the final result. The series we derive requires only 17 terms to ensure six or more significant figure accuracy for arguments in the range zero–six corresponding to error probabilities in the range $1/2$–10^{-9}. Meeting these criteria, the algorithm is also well suited for use on programmable pocket calculators and mainframe computers. Furthermore, the accuracy is easily extended in a manner described if greater precision is required.

Previously, a number of series approximations of $Q(\cdot)$ have been given in the literature. See, for example, [1]. These approximations are either only applicable in a restricted interval of argument, require several numerically precise coefficients, or require a great number of terms to converge for some values of argument [2]. For the same small number of terms, the relative error is significantly greater than for the series presented here. A family of upper and lower bounds and approximations of $Q(\cdot)$ has been presented in [2]. These give two–three accurate significant figures over the full argument range from zero to six. The magnitude of the relative error depends on the family parameters chosen, but is generally on the order of 10^{-1}–10^{-5} for this range. The magnitude of the relative error $Q(x)$ computed using the series presented here is less than 6.3×10^{-7} for all $0 \le x \le 6$ and is less than 1×10^{-10} for $0 \le x \le 4.47$.

The new series is derived in the next section.

II. DERIVATION OF THE SERIES

Let Y be a Gaussian random variable (R.V.) having zero mean and unit variance. Define the zero–one R.V. Z according to

$$Z = \begin{cases} 1, & y \ge x_0 \\ 0, & y < x_0 \end{cases} \tag{2}$$

where y represents a particular value of the R.V. Y and $x_0 \ge 0$ is a constant. Then

$$E[Z] = 0 \cdot P_r(Y < x_0) + 1 \cdot P_r(Y \ge x_0)$$
$$= E[U(Y - x_0)] = Q(x_0) \tag{3}$$

0090-6778/89/0900-0989$01.00