NOTICE

The quality of this microfiche is heavily dependent upon the quality of the original thesis submitted for microfilming. Every effort has been made to ensure the highest quality of reproduction possible.

If pages are missing, contact the university which granted the degree.

Some pages may have indistinct print especially if the original pages were typed with a poor typewriter ribbon or if the university sent us a poor photocopy.

Previously copyrighted materials (journal articles, published tests, etc.) are not filmed.

Reproduction in full or in part of this film is governed by the Canadian Copyright Act, R.S.C. 1970, c. C-30. Please read the authorization forms which accompany this thesis.

THIS DISSERTATION
HAS BEEN MICROFILMED
EXACTLY AS RECEIVED

AVIS

La qualité de cette microfiche dépend grandement de la qualité de la thèse soumise au microfilmage. Nous avons tout fait pour assurer une qualité supérieure de reproduction.

S'il manque des pages, veuillez communiquer avec l'université qui a conféré le grade.

La qualité d'impression de certaines pages peut laisser à désirer, surtout si les pages originales ont été dactylographiées à l'aide d'un ruban usé ou si l'université nous a fait parvenir une photocopie de mauvaise qualité.

Les documents qui font déjà l'objet d'un droit d'auteur (articles de revue, examens publiés, etc.) ne sont pas microfilmés.

La reproduction, même partielle, de ce microfilm est soumise à la Loi canadienne sur le droit d'auteur, SRC 1970, c. C-30. Veuillez prendre connaissance des formules d'autorisation qui accompagnent cette thèse.

LA THÈSE A ÉTÉ
MICROFILMÉE TELLE QUE
NOUS L'AVONS REÇUE

UNIVERSITÉ D'OTTAWA
UNIVERSITY OF OTTAWA

ON THE PROBABILITY OF UNDETECTED ERRORS

by

Efrain Guevara

A thesis submitted to the School of Graduate Studies,
University of Ottawa, in partial fulfilment
of the requirements for the degree of
Master of Applied Science.

Department of Electrical Engineering
Faculty of Science and Engineering
University of Ottawa
Ottawa, Canada

August, 1975

ACKNOWLEDGMENTS

The author wishes to gratefully acknowledge the guidance and encouragement of his supervisor, Prof. S.G.S. Shiva.

Thanks are due to Ronald Currie for the many stimulating discussions and useful suggestions. Thanks are also due to Tarek Abdel-Nabi for his helpful assistance with the computational procedures.

The author is grateful to the Defence Research Board and the National Research Council of Canada, who provided financial support under grant numbers DSB-9931-31 and A 3371 respectively.

TABLE OF CONTENTS

ABSTRACT

The problem of controlling the error occurrence in a communication channel is discussed. Two techniques for error control are presented : detection - retransmission and forward error correction. Of these two the detection-retransmission is a more suitable scheme for certain communication channels. Estimates are given for the probability of undetected errors when group error-correcting codes are used for error detection in the binary symmetric channel when the weight distribution of the code is unknown. The estimates presented are tight for small values of crossover probability p. It is seen that an improvement in the error-detecting ability is obtained by the use of even-weighted codes. Some examples of codes are presented for which the probability of undetected error Pe decreases with increasing crossover probability p.

CHAPTER 1

INTRODUCTION

Associated with the rapidly developing branches of modern sciences, there is a growing need to communicate, not only man to machine, but also between machines. Communication between machines employs electrical signals which may originate in analog form but before transmission they are transformed to digital form. The reasons for this transformation are that digital techniques [1] offer the advantages of increased accuracy, effective noise minimization and better processing, transmission and storage of information, whereas the accuracy of analog processed data becomes degraded after every operation and with greater operating speeds. Such degradation of accuracy does not occur with digital operation, since accuracy is a strict function of the number of digital bits.

One other attractive feature of digital techniques is that coding can be used to control errors.

Consider the simple communication system of Fig. 1.1 where the message is sent uncoded.

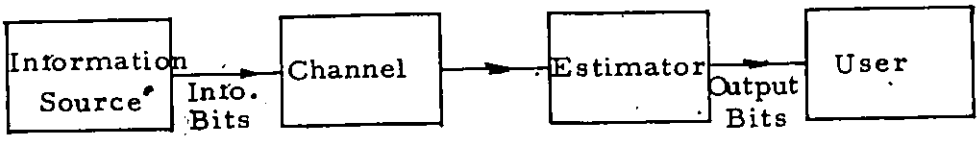

Figure 1.1

At the receiver an estimator attempts to recover the information from the output of the channel. The estimated sequence may or may not be correct. There exists the possibility that due to the distortion added by the channel noise, the output of the estimator is in error. Under these circumstances, the probability of error at the receiver is a function of the channel noise and the power of the signal.

For reliable operation, this probability of error must be kept as small as possible. One way of doing this is to increase the signal power up to a value for which the error rate at the receiver is acceptably low. Some systems, like short distance telephone communications, can afford to do this. But some others, like the satellite system, are power limited and the weight involved in providing increased power is too large. Again, in certain cases the channel is so noisy that the amount of signal power necessary for an acceptable reception is too large. In these cases, coding for error control can be used to reduce the error occurence.

Error-control coding attempts to guarantee that a digital transmission will be received with an error rate no greater than a prescribed value. Errors are detected and corrected through redundancy inserted in the messages. In this case, the probability of error is not only a function of the signal to noise ratio, but also of the characteristics of the code.

The advantage of coding is that for the same signal to noise ratio it reduces the error probability, or equivalently, for the same error probability a lower signal to noise ratio is required. This reduction in power required is called coding gain.

The simplest example of coding is replicate transmission, in which each bit of information is sent a minimum of three times to permit a majority decision at the receiving end. But for the amount of error protection it offers, replicate transmission wastes channel capacity. Better coding structures provide more complex interrelationships, thus giving greater capability for the correction or detection of errors, and make more efficient use of channel capacity.

There are two basic types of error control systems. The first, called detection-retransmission systems or automatic-repeat-request (ARQ), is illustrated in Fig. 1.2.

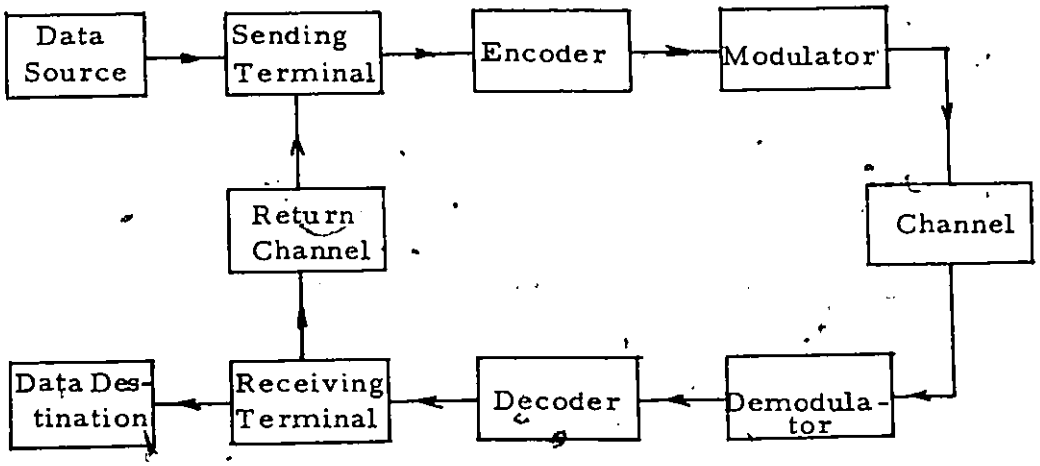

Figure 1.2 The ARQ System

In an ARQ system [2], [3] the sending terminal arranges the data in blocks, adds control and synchronization bits, and delivers the data blocks to the encoder which adds a number of parity bits according to a coding rule. These codes are known as block codes and are usually described using the notation (n, k) to indicate that the code contains n total bits in each block, of which k are information bits.

The encoder block is then delivered to the modulator and transmitted over the channel. At the receiving end, the block is demodulated and delivered to the receiving terminal through the decoder, which recomputes the parity bits from the received data and compares them with the received parity bits. If there are no discrepancies, the receiving terminal notifies the sending terminal through a return channel that the block has been correctly received. If discrepancies exist, the sending terminal is so notified and the block is retransmitted. With this system, erroneous data is delivered to the destination only if the decoder fails to detect the presence of errors.

The second technique for dealing with transmission errors can be represented by Fig. 1.2 with the reverse channel removed. The decoder is then a more complicated device that attempts to determine the location of the errors from the pattern of discrepancies between the received and the recomputed parity bits. This system, called forward error correction (FEC) [4], requires a redundancy considerably higher than that for error detection, for the same degree of protection against errors. With this system, erroneous data is delivered to the user whenever the decoder cannot determine the exact location of the errors.

In either system, error detection or error correction, a relevant property of the code used is its minimum distance d. The minimum distance can be defined as the minimum number of errors that must be made in a block, to change one code word into another. Maximum error-correction or detection capability of a code is obtained by making the minimum distance between codewords as large as possible for a given code length and redundancy. If a code has minimum distance d, it can correct $t = \frac{d-1}{2}$ errors or fewer or when used for error detection, it is guaranteed to detect up to (d-1) errors.

Depending on the nature of the error patterns expected on the channel, codes for FEC systems may be designed to correct a maximum number t of random errors (i.e. independent errors) or a burst error of length b. By a burst of length b we mean a span of b bits, beginning and ending with an error. Each of the b-2 bits in the interior of a burst may or may not be in error. Block codes have also been designed to correct combinations of random and burst patterns, usually called "compound" errors.

There is another class of codes, called convolutional codes [5], in which the check bits are scattered among the information bits but there is no fixed block structure. Convolutional codes, like block codes, can be used either to detect or correct errors. However, because data is usually retransmitted in blocks, block codes are better suited for error detection applications. We do not consider convolutional codes in this thesis.

A hybrid scheme [6] consisting of an FEC system contained within an ARQ system can also be used for error control. In this scheme, part of the error-correcting capability of the code is used to correct certain error patterns, while the other part is used to detect errors. In the case of correction of t' errors that is less than the error correcting capability t, the code has an error-detecting ability D given by $d = t' + D + 1$, where $D > t'$.

Theoretical results [7] have shown that when a hybrid scheme is used in the binary symmetric channel (BSC) with crossover probability $P > 10^{-4}$, a probability of undetected bit error of less then 10^{-9} can be achieved by correcting only a few errors while retaining a reasonable throughput and a very low retransmission rate. Another

study of the performance of hybrid scheme on satellite channels [8] shows that this scheme offers substantial improvement in throughput efficiency over either ARQ or FEC systems in such channels.

The circuitry required for the encoder of either error-correcting or error-detecting systems is quite simple. For cyclic codes, all that is required [9] is a shift register of length k or (n-k), whichever is shorter, and about half that number of exclusive OR gates. For the (1023, 1013) Hamming code a ten-bit shift register and two exclusive OR gates are sufficient. But the decoder for error-correcting can become extremely complicated and costly. For example Peterson's procedure for decoding BCH codes [10] requires a decoder that increases in size and speed as $n \log_2 n$. Error detection circuitry is simple at both the encoder and the decoder. (A code with n-k parity check bits requires a decoder with only two (n-k)-bit shift registers and about $\frac{n-k}{2}$ exclusive OR gates [6]). This is because the decoder need simply re-encode the received information bits and compares the parity bits thus generated with the received parity bits. Any discrepancy indicates an error.

Our main concern in this thesis will be error detection rather than error correction.

The probability of an undetected error Pe, gives a measure of the goodness of the (n, k) error detecting code. Given the sum of a codeword and an error, the decoder detects an error if and only if the sum is not a codeword. The sum can be a code word if and only if the error pattern is a codeword. If the channel under consideration is a BSC with crossover probability p, Pe is given by [11]

$$Pe = \sum_{i=d}^{n} Ai\, p^{i} (1-p)^{n-i} \qquad (1.1)$$

where the Ai's denote the number of code words of weight i in the (n, k) code. The numbers Ai, i = 0, 1, 2,.....n, form the weight distribution or weight spectrum of the code.

From equation (1.1) we see that in order to compute Pe, the weight distribution of the code must be known. Weight distributions are known for a handful of codes only. Finding them in many cases is a complicated affair.

THESIS OUTLINE

In this work we are concerned with the problem of computing the probability Pe of undetected errors, when random-error-correcting binary group codes are used for detection only, in binary symmetric channels with cross-over probability p.

In chapter 2 we discuss the nature of errors on a data communication system and the basic techniques for dealing with these errors. We compare these techniques and conclude that detection-retransmission systems are better suited to the task than forward error control systems.

In chapter 3 we develop various estimates of Pe for group codes. For these codes containing the code word of all ones, we refine these estimates. Plots of Pe and their estimates are presented for some 30 codes for which the weight distributions are known. We also show that if the even-weighted subset of a code is used for error detection, Pe can be substantially reduced.

In chapter 4 we present some codes with an interesting property observed in the process of this study, the property being that contrary to the intuitive feeling that Pe should decrease as the signal to noise ratio decreases, for these codes Pe can actually increase with an increase in signal to noise ratio.

Finally in chapter 5, conclusions and recommendations for further work are presented based on the results of this study.

CHAPTER 2

ERROR STATISTICS AND ERROR CONTROL

2.1 INTRODUCTION

The error occurrence on communication systems is inevitable and very difficult to describe. Usually these difficulties are ignored and the performance of transmission equipment is specified in terms of error rates measured in laboratory tests assuming white Gaussian noise only. Unfortunately conditions in the real world are very much different. Errors are produced by a variety of causes in addition to Gaussian noise, including fades in microwave facilities, impulses caused, for example, by lightning or by central-office switching equipment, etc. For the telephone channel, the average error rate for medium speed transmission is 10^{-5}. For some applications, this may be acceptable ; others would require better accuracy and error control becomes then necessary.

In order to design the error control system, we must know how the errors occur. Several surveys [12] - [15] have been conducted by the Bell System to establish the data transmission error performance on the telecommunication network. One of the recent surveys, known as the 1969-1970 Connection Survey [15] , presents results based on measurements made on about 600 toll connections, dialed from 12 receiving to 92 transmitting sites in the United States and Canada. In the next section we will briefly state the results of this survey which are meaningful in evaluating error control systems and comment on some attempts to model these error statistics.

2.2 ERROR STATISTICS : THE 1969-1970 CONNECTION SURVEY

Several modems were tested at 1200, 2000, 3600 and 4800 b/s using a 511-bit pseudo-random word as the data source. The statistics were presented in terms of cumulative distribution functions for bit error rates, burst rates and block error rates.

Average bit error rates for all calls are presented in Figures 2.1 and 2.2. These figures show cumulative distribution functions of the bit error rate per call for operation at 1200 and 3600 b/s in the short, medium and long mileage strata. The mean error rate for all calls for both 1200 and 3600 b/s was slightly better than 10^{-4} errors/bit transmitted. But because the error rate distributions are skewed, the mean error rates are largely determined by the worst-case calls. For example for all of the calls measured at 2000 b/s, 72% of the errors occurred on that 5% of the calls which had the poorest error rate. In fact from Figures 2.1 and 2.2 we can see that for both cases, more than 80% of the connections had better than average error rates (10^{-4} errors/bit).

Errors on telephone channels tend to occur in bursts, and since bit error rates are not sufficient to characterize this property, burst and block rates are necessary. In these results, an error burst is defined to be a collection of one or more bits beginning and ending with an error and separated from neighboring bursts by 50 or more error-free bits. Block error rate is the probability of a block being received in error. Figures 2.3 and 2.4 present the cumulative distribution functions of total burst, bit and block error rate for block sizes of 100, 500, 1000, 5000 and 10000 bits for data rates 2000 and 4800 b/s . These distributions were formed by averaging the distributions for short, medium and long mileage strata assuming equal weight in each mileage

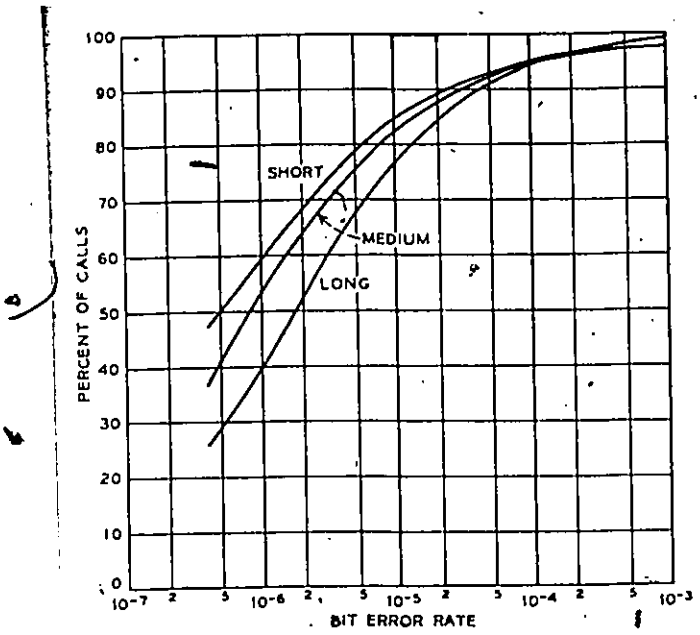

Figure 2.1 Bit error rate distributions by mileage strata at 1200 b/s

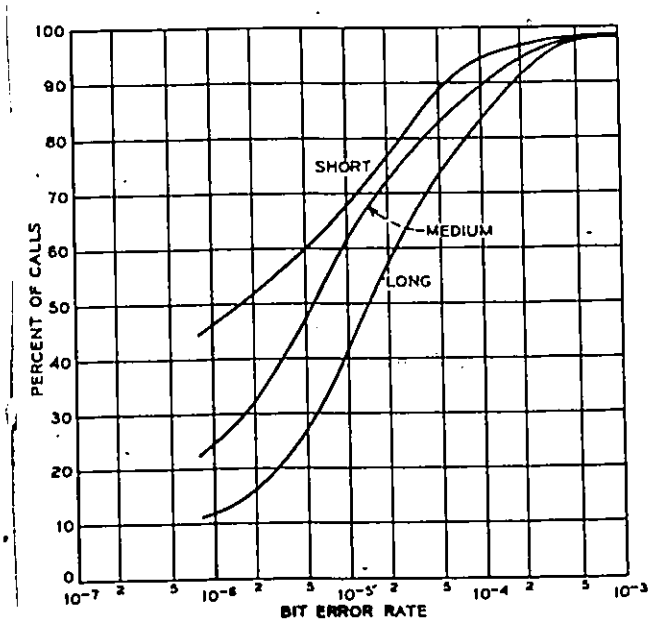

Figure 2.2 Bit error rate distributions by mileage strata at 3600 b/s.

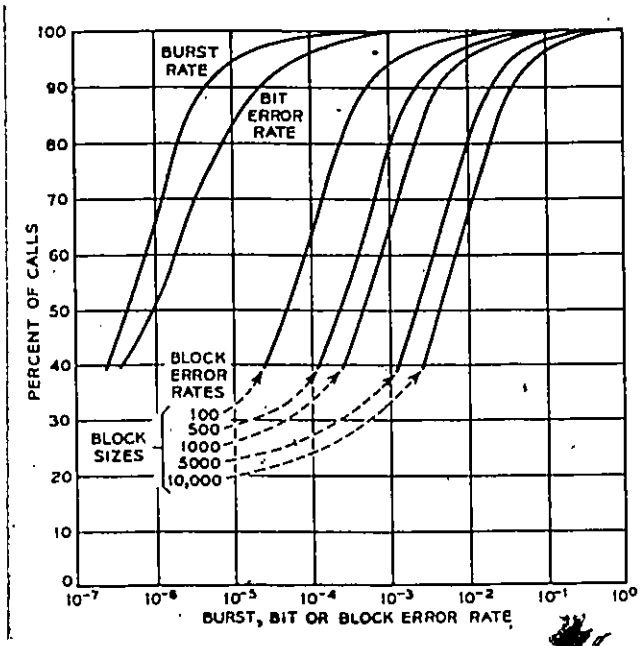

Figure 2.3 Total burst, bit and block error rate distributions at 2000 b/s (Each mileage band weighted equally).

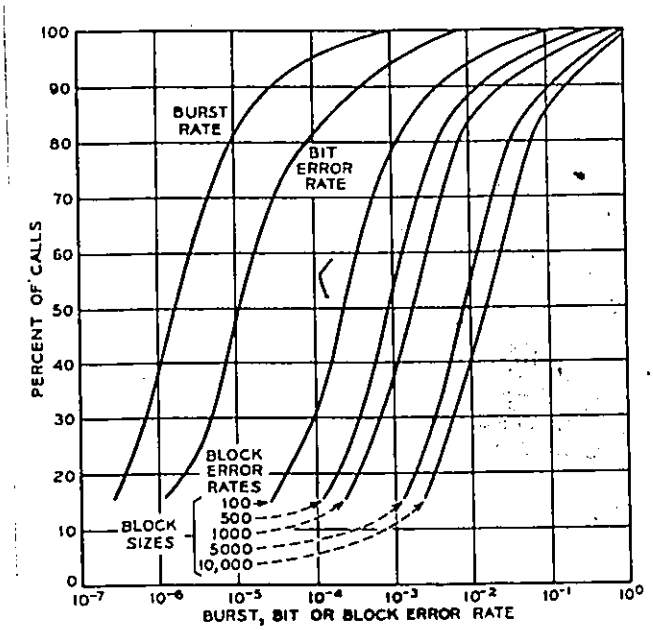

Figure 2.4 Total burst, bit and block error rate distributions at 4800 b/s (Each mileage band weighted equally).

category. A further characterization of error burst is given by Fig. 2.5 which shows the probability distribution of burst lengths. (A burst length is defined to be the number of bits in a burst).

Finally another result of this survey useful for evaluation of error control systems is the probability of m or more errors in a block of n bits. [P ($\geq$ m, n)]. For considerations to follow, we present in Fig. 2.6 the results for a 2000 b/s system.

From these statistics, it is clear that errors are not independent randomly distributed events. In fact, it is concluded that impulse noise is the principal source of errors and these errors tend to appear in bursts. Another conclusion that may be drawn from this and previous surveys is that error rates are not mileage or speed related in a way that significantly influences error-control procedures. Now we will give some examples of how these error statistics can be useful in evaluating error-control systems [16].

Suppose that an ARQ system is chosen for error control. Once the system has been specified, the only variables affecting the effective data rate or throughput T is the block error probability Pe (block). Block error probabilities are presented in Figures 2.3 and 2.4. This data and data from other earlier field tests of voice-band modems indicate that the probability of a block error can be approximated by a constant times the block length n. For example Fig. 2.6 shows Pe (block) for a 2000 bit/s system. The curve for P($\geq$ 1,n) = Pe (block) can be approximated by Pe (block) $\approx$ 4×10^{-6} n. Thus simple comparisons of retransmission strategies for different block lenghts can be obtained using Pe(block) $\approx$ a. n.

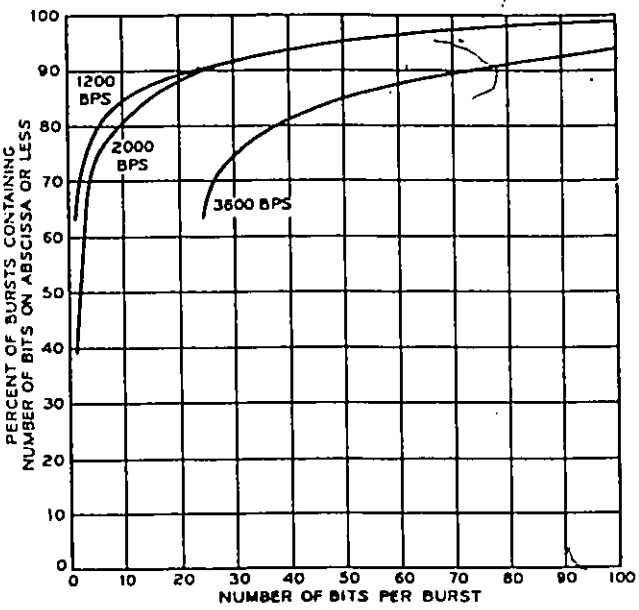

Figure 2.5 Burst length distributions.

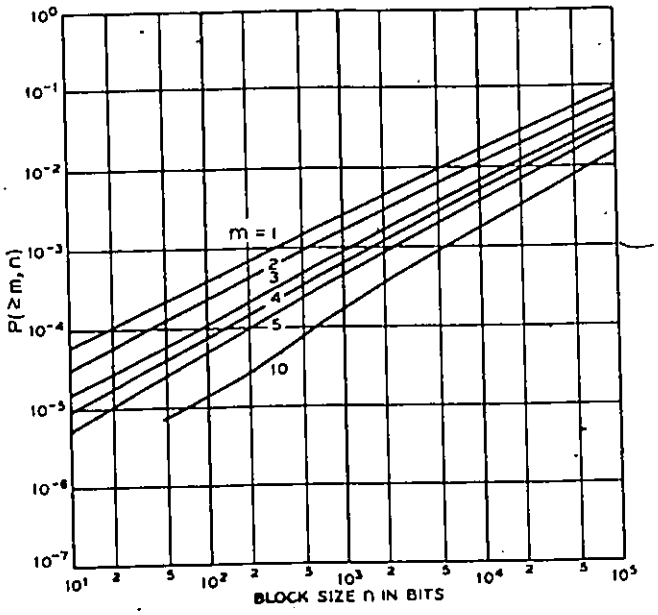

Figure 2.6 Probability of m or more errors in a block of size n [P (≥ m, n)] .

Derivations of approximations for FEC systems can become more complicated. However from the statistics presented it is easy to observe that average bit error rate is not going to be reduced much with random error correcting codes. For example, referring to Fig. 2.6 again, if n = 100 the probability of a block error is about 4×10^{-4}, but the probability of a block with more than 4 errors is just slightly less than 10^{-4}. Thus an error-correcting code with n = 100 and d = 10 would fail to correct $\frac{1}{4}$ of the blocks in error. If the same code were used for error-detection, the decoder would fail to detect only those blocks with more than 9 errors and only when those errors have changed the received block into a different code word. If the same code were used to correct error in a channel with errors that are independent randomly distributed with a bit error rate of 10^{-4}, we have from the Gaussian distribution that $P(\geq 5, 100) \approx 10^{-12}$ and therefore it would be very effective.

The statistics show that errors are correlated. Burst-error-correcting codes are constructed taking into account this condition. For such codes to be effective, the length of the burst must not exceed b bits. Unfortunately telecommunications channels do not conform to such a burst model any better than to the random error model. For example Fig. 2.5 shows burst length distributions for a guard-space length of 50 bits. An optimum burst-error-correcting code with rate $\frac{b}{n} = \frac{1}{2}$ and a guard space of 50 bits can correct error bursts of length up to 16 bits. From the figure and the 2000 bit/s curve, we see that about 15% of the bursts have lengths greater than 16 bits.

From these examples we see that random-error or

burst-error-correcting codes are not suited to telephone data applications. The fact is that when one attempts to model a communication system, the less frequent or atypical error events are likely to be estimated poorly and it is just such events that lead to uncorrected errors.

In the next section, we consider the merits of ARQ and FEC systems.

2.3 DETECTION - RETRANSMISSION vs FORWARD ERROR CONTROL

Detection-retransmission (ARQ) systems and FEC systems have been compared extensively both on real telephone channels and with theoretical models [17], [2], [3]. In every case the results have demonstrated the superiority of detection-retransmission systems.

Fontained and Gallager [17] (1961) compared the two systems on the real telephone channel. They concluded that FEC systems are impractical for the telephone channel since the capabilities of such schemes are overloaded during the noisy periods and wasted at other times. They also show that error-detecting schemes with moderate size block lengths (100 to 500 symbols) and a small amount of redundancy (15 to 20 symbols) are capable of reducing the probability of undetected errors to negligible values.

Benice and Frey Jr. [3] in 1964, compared several error-control systems in theoretical models for channels exhibiting independent and dependent errors. The results showed that for independent errors, forward error control provides substantial improvement over retransmission for high bit-error probabilities, provided that extremely high reliability is not required.

For dependent errors, retransmission was always superior in throughput and always considerably superior in undetected error probability.

From these studies we conclude that the nature of the errors in the channel is by far a more critical problem in the design of FEC systems than it is for ARQ systems. ARQ systems are relatively

insensitive to the conditions on the channel. This results from the fact that if the number of parity bits is n-k, the fraction of undetectable error patterns is approximately $\frac{1}{2^{n-k}}$ regardless of the length of the code [17]. It follows that since a code can be easily chosen to detect the vast majority of all error patterns, it does not matter very much how errors occur on the channel. For example, a code used by IBM in many of their computer communications systems [18], has 16 parity check bits and is capable of detecting all blocks with 3 errors or less or with burst patterns of length b = 16 bits or less, provided the block length is less than $2^{15}-1$. With a block length of 800 bits, the probability of having an undetected error with this code has been pessimistically estimated at 10^{-8} [19].

This advantage of ARQ systems is not shared by FEC systems. Of all the errors detected by an error correcting code only a small fraction ($\frac{1}{2^k}$ at most, where k is the number of information bits) are correctable. This is illustrated in Fig. 2.7 where the 2^n n-tuples are divided into cosets.

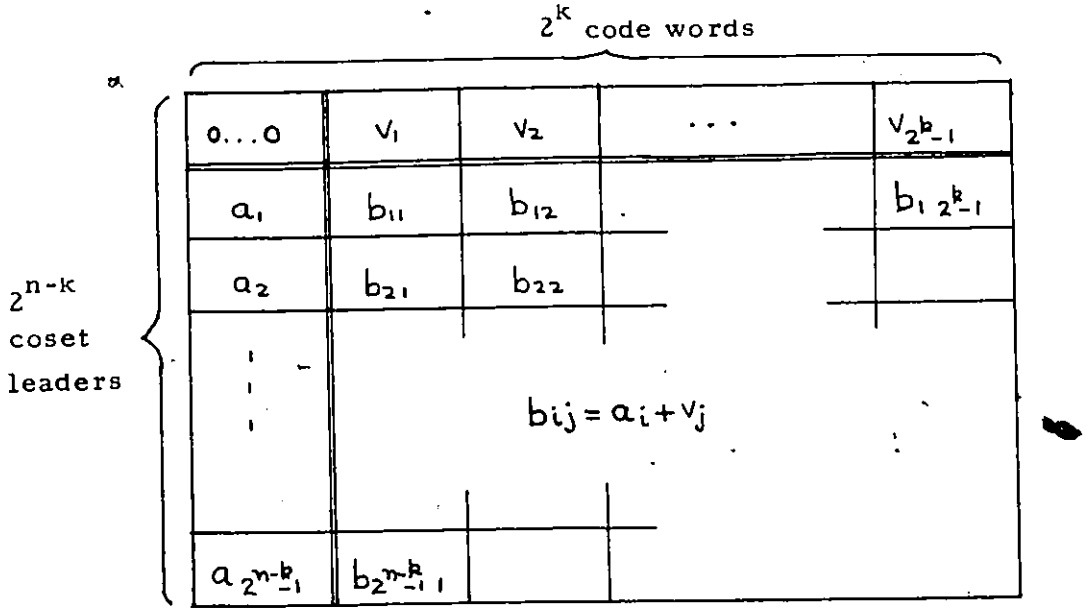

Figure 2.7

In this figure the detectable error patterns are the a_i's and the b_{ij}'s, while the correctable patterns are only the a_i's or coset leaders. Error-correcting codes are therefore most effective in channels for which it is possible to choose as coset leaders the most probable error patterns. This implies that the behavior of the channel is predictable and not subject to macroscopic changes. The telephone channel cannot be relied upon to be so well behaved, but there are other channels that comply with this characteristic. Fortunately the satellite channel is an example, since in this case retransmission implies a large delay and becomes impractical for such an application. There are other situations in which retransmission is not possible and FEC becomes mandatory. Disc storage systems is an example [20]. Modern disc drives have packing densities of 4000 bits per inch and 200 tracks per inch. Errors are caused by imperfections in the magnetic coating of the disc and affect more than one bit at a time. A code used in this application is the (139 197, 139 118). Fire code which can correct bursts up to 11 bits long. This code was chosen because it allows the encoding of 1 track per block on the average, and it was experimentally found that surface imperfections seldom affect more than 11 bits.

Unfortunately, forward error correction is complex compared to detection-transmission. The problem of obtaining simple algorithms for error correction has been the subject of a considerable amount of research [4], [21], [22]. Recent developments in error-correcting codes for the telephone channel [23] indicate that FEC systems can improve reliability and that such codes may be useful in applications where retransmission is impractical.

2.4 ARQ SYSTEMS

One important aspect of ARQ systems is the effective rate at which information is transferred from source to destination. In this section we will discuss the dependence of this rate on the channel error statistics and on the type of retransmission system [16]. There are two systems of retransmission that are used: stop-and-wait and continuous-retransmission.

2.4.1 STOP-AND-WAIT ARQ SYSTEM

This is the simplest and most used detection - retransmission system [2].

In stop-and-wait operation the transmitter sends a block and waits for a positive or negative acknowledgment from the receiver before sending the next block or retransmitting the same block. The effective throughput T of such a system is given by [24]

$$T = \frac{n(1 - Pe(block))}{n + c \cdot \nu} \qquad (2.1)$$

where c is the time delay from the transmission of one block to the beginning of transmission of the next, and ν is the signaling rate of the modem. (Here, perfect synchronization is assumed). The effective information rate is then given by

$$Re = T\nu \qquad (2.2)$$

From equation (2.1) we can see that T, and hence Re is degraded whenever Pe (block), or the round-trip delay, $c \cdot \nu$, become appreciable. The block length n should be made large relative to the delay; in fact, the use of short block lengths for certain applications, may result in very inefficient operation even when there are no errors in the received data. For example, consider a direct-distance-dialed (DDD)

coast-to-coast connection. The time delay has been estimated at 360 m sec., including the turnaround time taken in changing the half-duplex modem from one direction to the other. Hence, for example on an error free channel with ν = 4800 b/s and using a block length of 1000 bits, Re = 1760 b/s, which is only about 37% of the modem rate. Therefore in this application a longer block length should be used. For example, if n = 10,000 bits and the channel is error free, Re = 4100 b/s, about 85% of ν. In the light of the example, higher speed modems will yield very little improvement on Re if n is not increased appropriately. But, if n is made too large, Pe(block) could become significant enough to cut down the throughput T. It is likely, however, that such higher speed modems will be used primarily on private lines. Since full-duplex operation is then possible, there is no delay associated with channel turnaround and the time delay is reduced substantially.

If satellites are used in the transmission links, the delay more than doubles and the efficiency of the system drops about 10%. For example the round trip propagation delays for satellite links have been estimated at 540 m sec [24] Thus if we allow 150 ms to reverse the transmission direction on a DDD facility, $\dot{c}$ = 540+300 = 840 m sec. On an error free channel, if n = 10000 bits and ν = 4800 b/s, Re = 3410 b/s, that is about 72% of the modem rate.

Thus, stop-and-wait ARQ systems are inherently inefficient due to the idle time spent in acknowledgments and retransmissions. This inefficiency, while not serious on most present systems, may become unacceptable on systems which employ higher modem speeds or satellite links.

2.4.2 CONTINUOUS ARQ SYSTEM

In continuous detection-retransmission [2], [3], the sending terminal does not wait between blocks for acknowledgments, but continues sending blocks until a retransmission of a given block is requested. At this point the transmitter goes back and retransmits that block and all blocks transmitted from that point and the receipt of the retransmission request.

The minimum number of blocks that must be retransmitted is given by $x + 1$ where $x = \lfloor (c \cdot \nu)/n \rfloor + 1$ ($\lfloor y \rfloor$ means the integer part of y). Assuming that the transmitter always completes the present block before initiating a retransmission, the throughput T can be lower bounded by

$$T \geq \frac{1 - Pe\ (block)}{1 + x\,Pe\ (block)} \qquad (2.3)$$

When used in the satellite channel, a continuous ARQ system is much more efficient than a stop-and-wait system.

As an example, consider a DDD satellite connection. Here, the delay c is estimated at about 750 m sec. Suppose $\nu = 4800$ b/s and $n = 5000$ bits; then $x = 1$. At the 90% point on the appropriate curve of Figure 2.4, $Pe\ (block) = 10^{-1}$ and $Re \geq 3930$ b/s. At the 50% point, $Pe\ (block) = 9 \times 10^{-3}$ and $Re \geq 4710$ b/s.
If we let $n = 1000$, then $x = 4$. Thus for the 90% case, $Pe(block) = 3 \times 10^{-2}$ and $Re \geq 4150$ b/s while for the 50% case $Pe(block) = 2 \times 10^{-3}$ and $Re \geq 4750$ b/s. This example, which uses actual data, shows the superiority of continuous ARQ systems. It is also interesting to note that in contrast to the stop-and-wait ARQ system, the efficiency of the continuous ARQ system generally increases as the block length is

decreased.

One disadvantage of this system, however, is that it requires full-duplex operation (i.e transmission should proceed in both directions), and almost all systems today operate in a half-duplex mode (i.e they cannot transmit and receive simultaneously). This is the reason why, despite its superiority in terms of efficiency, continuous retransmission systems are almost nonexistent at present in practice.

In concluding we can say that while the present ARQ systems may not be satisfactory for future demands of the telecommunication channel, the solution lies not in FEC systems but in a better ARQ technique.

CHAPTER 3

ESTIMATES FOR THE PROBABILITY OF UNDETECTED ERRORS

3.1 - UPPER BOUNDS ON Pe

As stated earlier, the probability Pe of an undetected error is a measure of the goodness of the error detecting code. The performance of any code can be specified by a graph of the expected Pe vs. signal to noise ratio. Pe depends on the nature of the errors caused by the channel and the weight distribution of the code used. In this analysis we will consider the binary symmetric channel (BSC) with cross-over probability p. Let V be a binary (n,κ) group code with minimum distance d, and let A_i be the number of code words of weight i.

Given the sum of a codeword and an error, the decoder does not detect an error if and only if the sum is a codeword. Otherwise it detects the error. Therefore the decoder fails to detect errors whenever the noise added by the channel is a codeword, and the probability of this event is given by

$$Pe = \sum_{i=d}^{n-1} A_i p^i (1-p)^{n-i} + A_n p^n . \qquad (3.1)$$

With respect to (3.1), if we restrict p to the range $o \leq p \leq \frac{1}{2}$, the ratio

$$\frac{p^{i+1}(1-p)^{n-i-1}}{p^i (1-p)^{n-i}} = \frac{p}{1-p} \leq 1 , \qquad (3.2)$$

which means that the first term of the binomial expansion of (3.1), i.e.

$p^d (1-p)^{n-d}$ is the largest. An upper bound on Pe can be obtained by replacing all the binomial terms of the expansion of (3.1) by the largest of them, $p^d (1-p)^{n-d}$:

$$Pe \leq B_1 = p^d(1-p)^{n-d} [A_d + A_{d+1} + \ldots + A_{n-d}] + A_n p^n$$

$$Pe \leq B_1 = p^d(1-p)^{n-d} (2^k - 2) + p^n \qquad (3.3)$$

We note that $B_1 = Pe$ for $p = \frac{1}{2}$ and for the case when all the words in the code have the same weight such as the MLSR codes.

The bound B_1 is plotted for certain codes in Figures 3.1 to 3.7. We observe that for large values of p, $p \neq 1/2$, B_1 is a loose bound although in some cases (Figs. 3.1, 3.2 and 3.7) it is within one decade from Pe. For a given weight distribution, as p gets smaller, B_1 becomes a better bound .

This upper bound can be improved if it is known that the code contains the word of all ones, since in that case we can write :

$$Pe = A_d p^d (1-p)^{n-d} + \ldots + A_{\frac{n-1}{2}} p^{\frac{n-1}{2}} (1-p)^{\frac{n+1}{2}} +$$

$$+ A_{\frac{n+1}{2}} p^{\frac{n+1}{2}} (1-p)^{\frac{n-1}{2}} + \ldots + A_{n-d} p^{n-d} (1-p)^d + p^n .$$

Since $p^d(1-p)^{n-d} > p^{d+1}(1-p)^{n-d-1} > \ldots > p^{\frac{n-1}{2}} (1-p)^{\frac{n+1}{2}}$

and $p^{\frac{n+1}{2}} (1-p)^{\frac{n-1}{2}} > p^{\frac{n+3}{2}} (1-p)^{\frac{n-3}{2}} > \ldots > p^{n-d} (1-p)^d$

we can write

$$Pe < p^d(1-p)^{n-d} [A_d + A_{d+1} + \ldots + A_{\frac{n-1}{2}}] +$$

$$+ \; p^{\frac{n+1}{2}} (1-p)^{\frac{n-1}{2}} \left[A_{\frac{n+1}{2}} + A_{\frac{n+3}{2}} + \ldots + A_{n-d} \right] + p^n$$

$$\text{or } Pe < p^d (1-p)^{n-d} (2^{k-1}-1) + p^{\frac{n+1}{2}} (1-p)^{\frac{n-1}{2}} (2^{k-1}-1) + p^n = UB \qquad (3.4)$$

UB is plotted for the (15,7) d = 5, BCH code in Fig 3.8 . Comparing this bound with B_1 in Fig 3.2 for the same code, we see that for all values of $p < \frac{1}{2}$, UB is smaller than B_1. For small values of p, the value of UB tends to $\frac{B_1}{2}$. This is to be expected since UB consists of a term equal to $\frac{B_1}{2}$ added to a term which tends to be much smaller than $\frac{B_1}{2}$ for small values of p, as long as $d < \frac{n+1}{2}$.

Example 3.1

Consider the (41,21) d = 9, BCH code and a BSC with p = 0.01.

Then

$$B_1 = p^9(1-p)^{32}(2^{21}-2) + p^{41} = 1.523093 \times 10^{-12}$$

$$UB = p^9(1-p)^{32}(2^{20}-1) + p^{21}(1-p)^{20}(2^{20}-1) + p^{41}$$

$$= 7.60196255 \times 10^{-13}$$

$$UB \approx 1.523093 \times 10^{-12} = B_1$$

In this case $d \approx \frac{1}{2}\left(\frac{n+1}{2}\right)$.

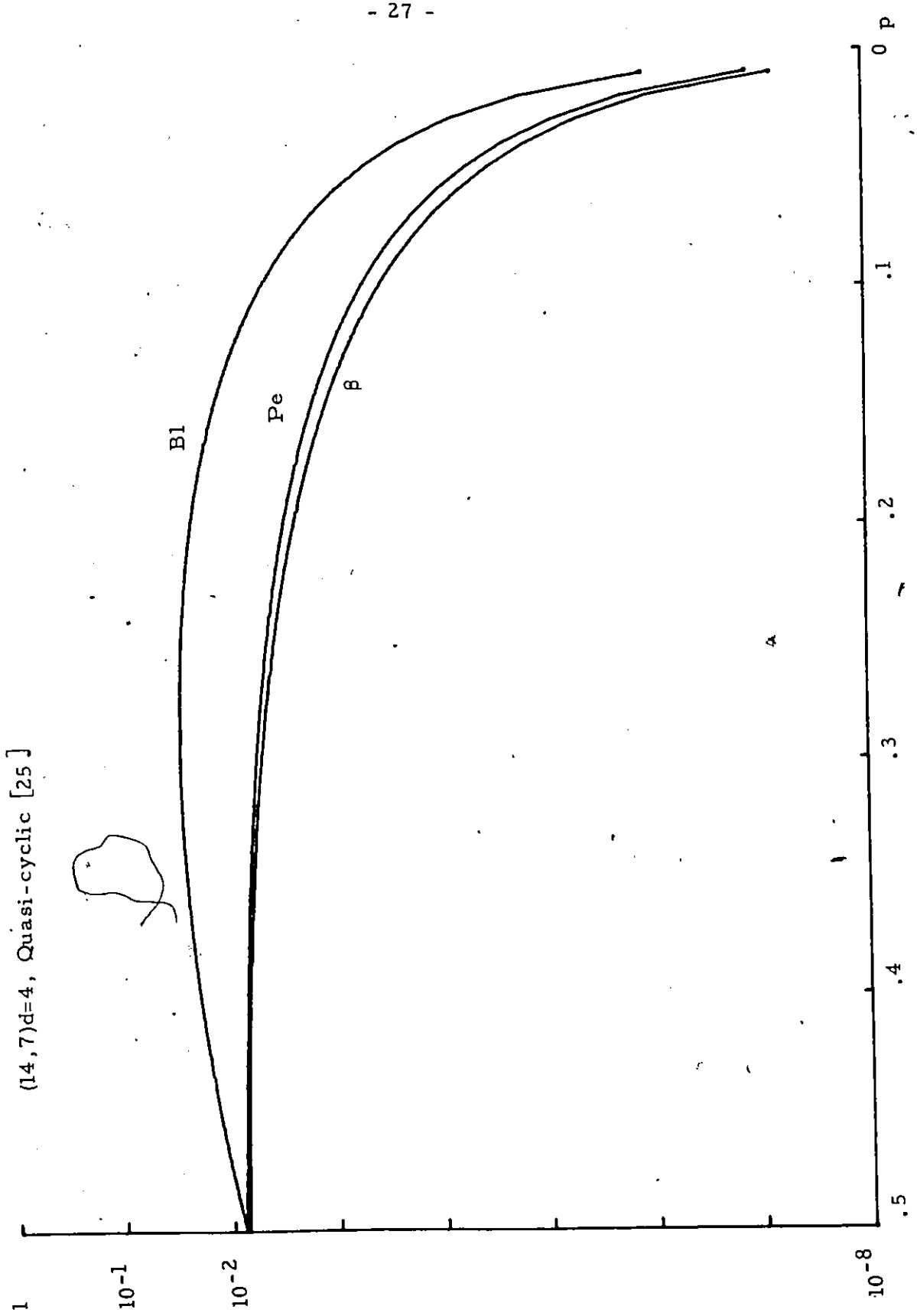

Figure 3.1

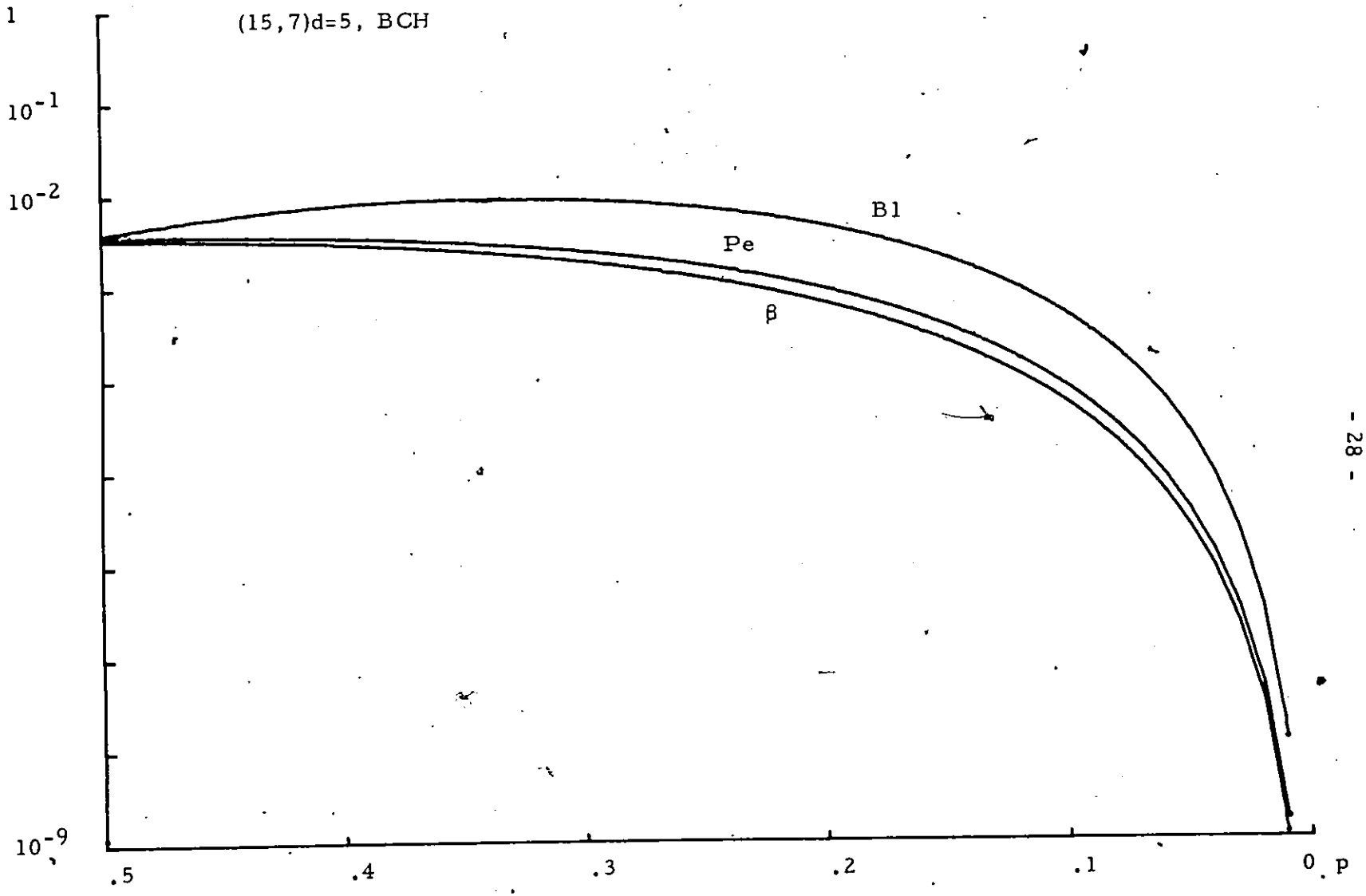

Figure 3.2

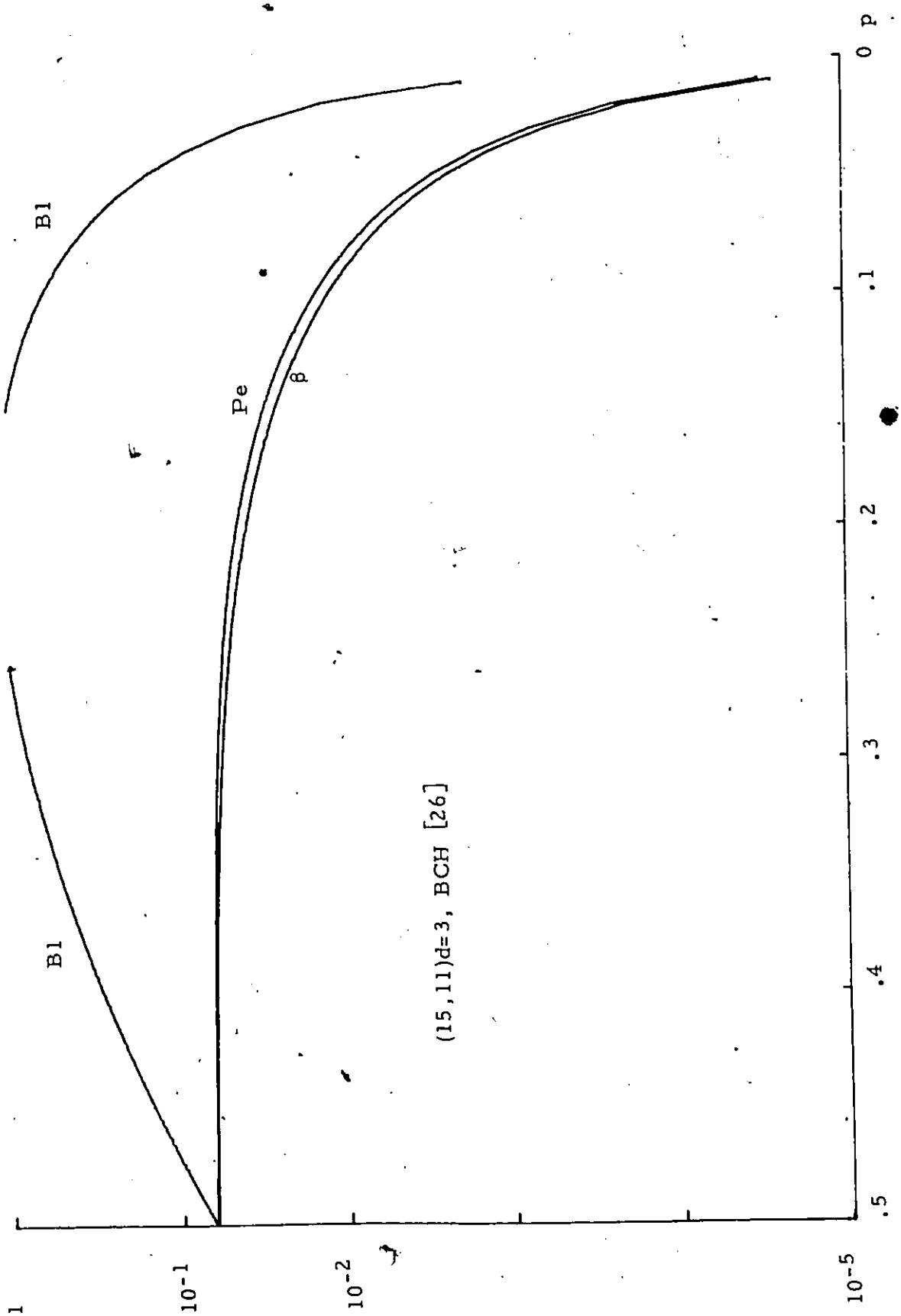

Figure 3.3

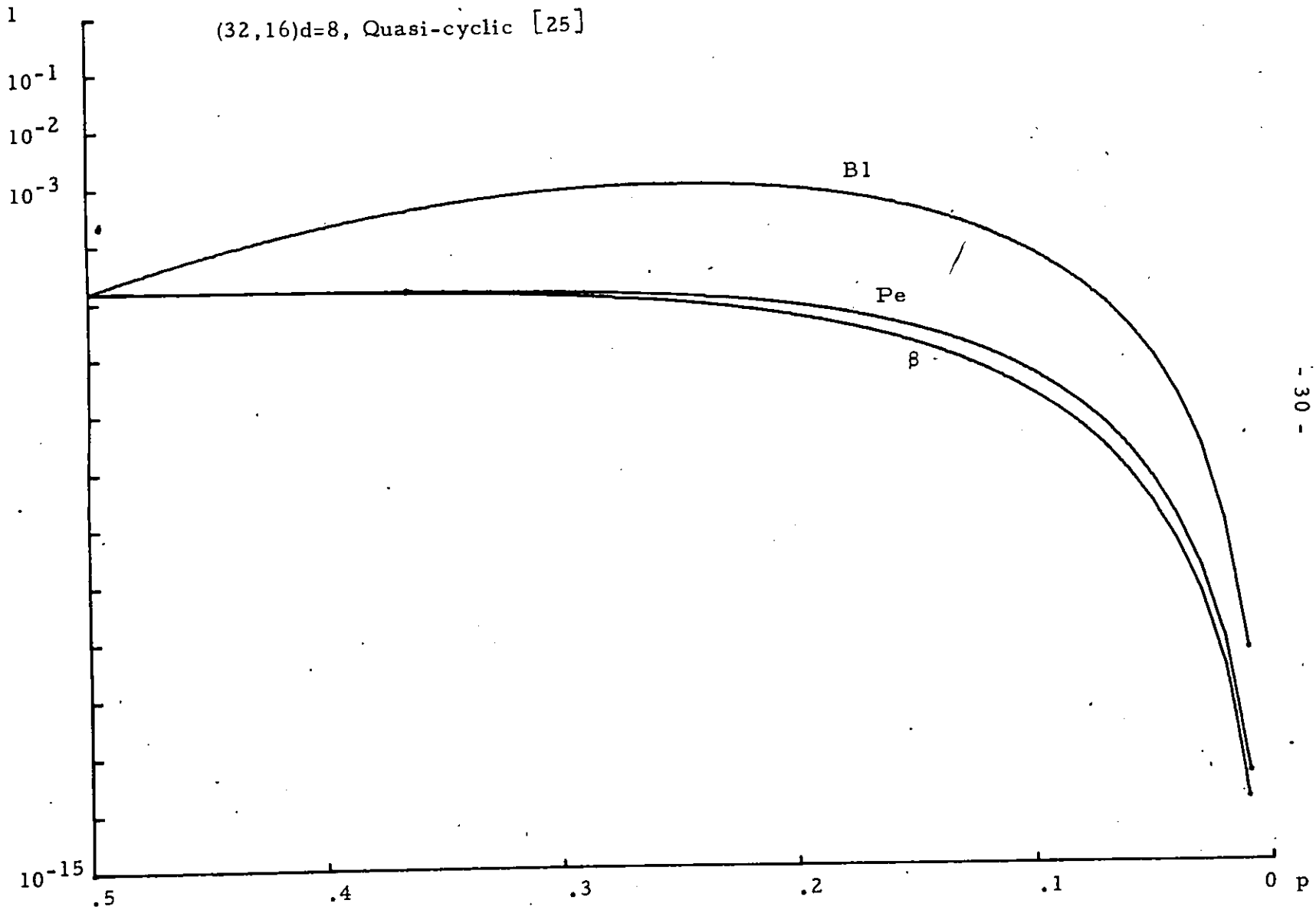

Figure 3.4

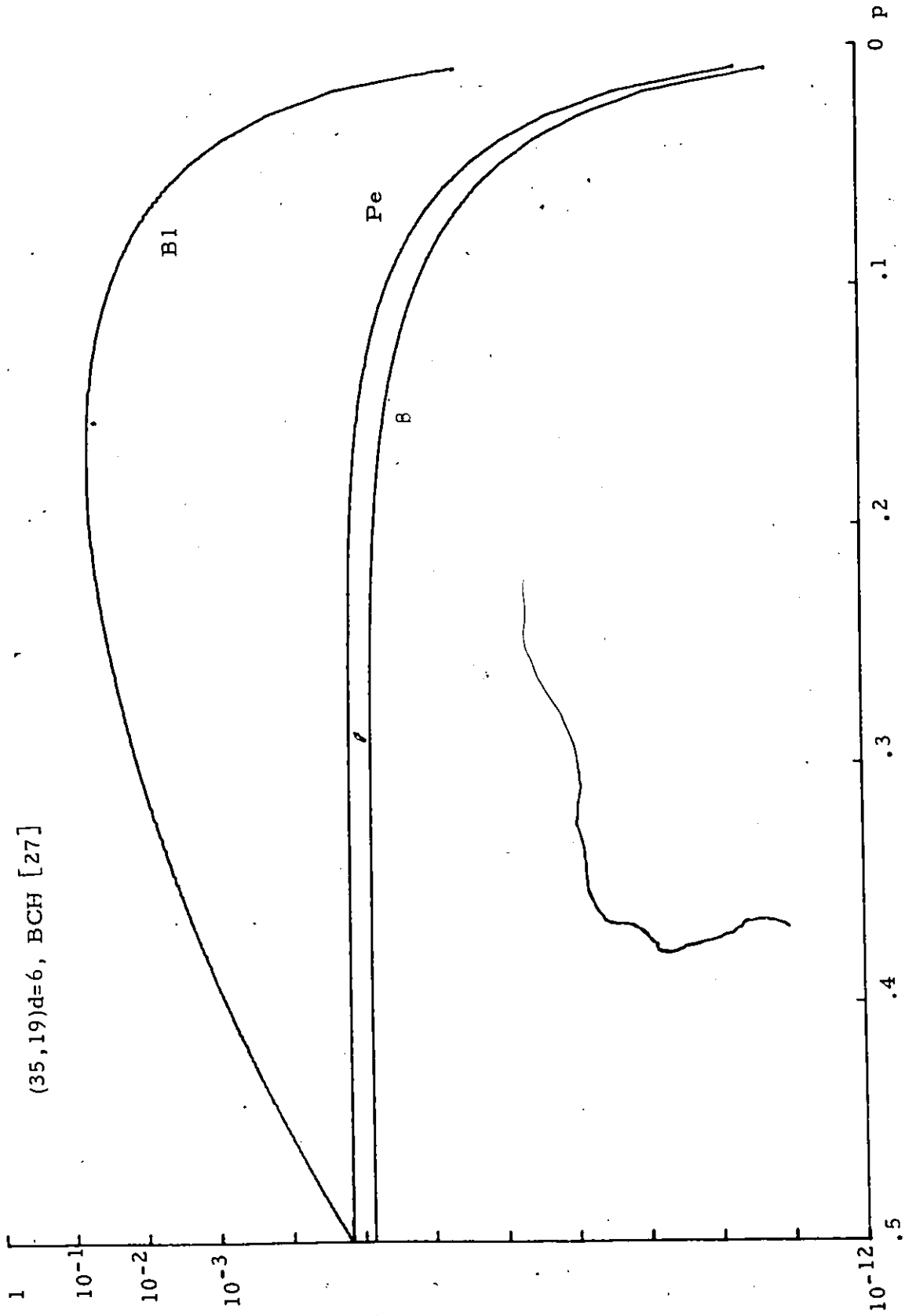

Figure 3.5

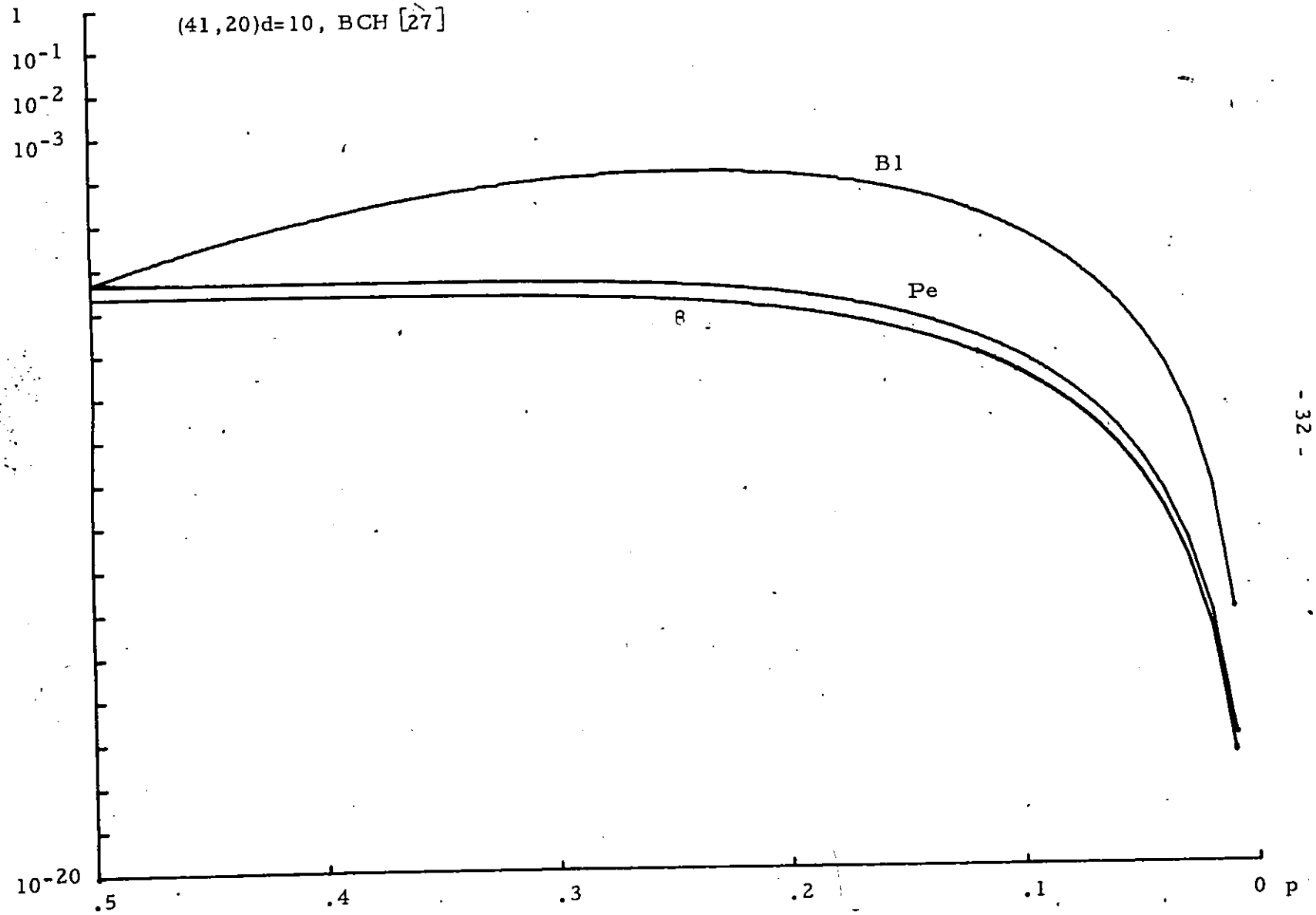

Figure 3.6

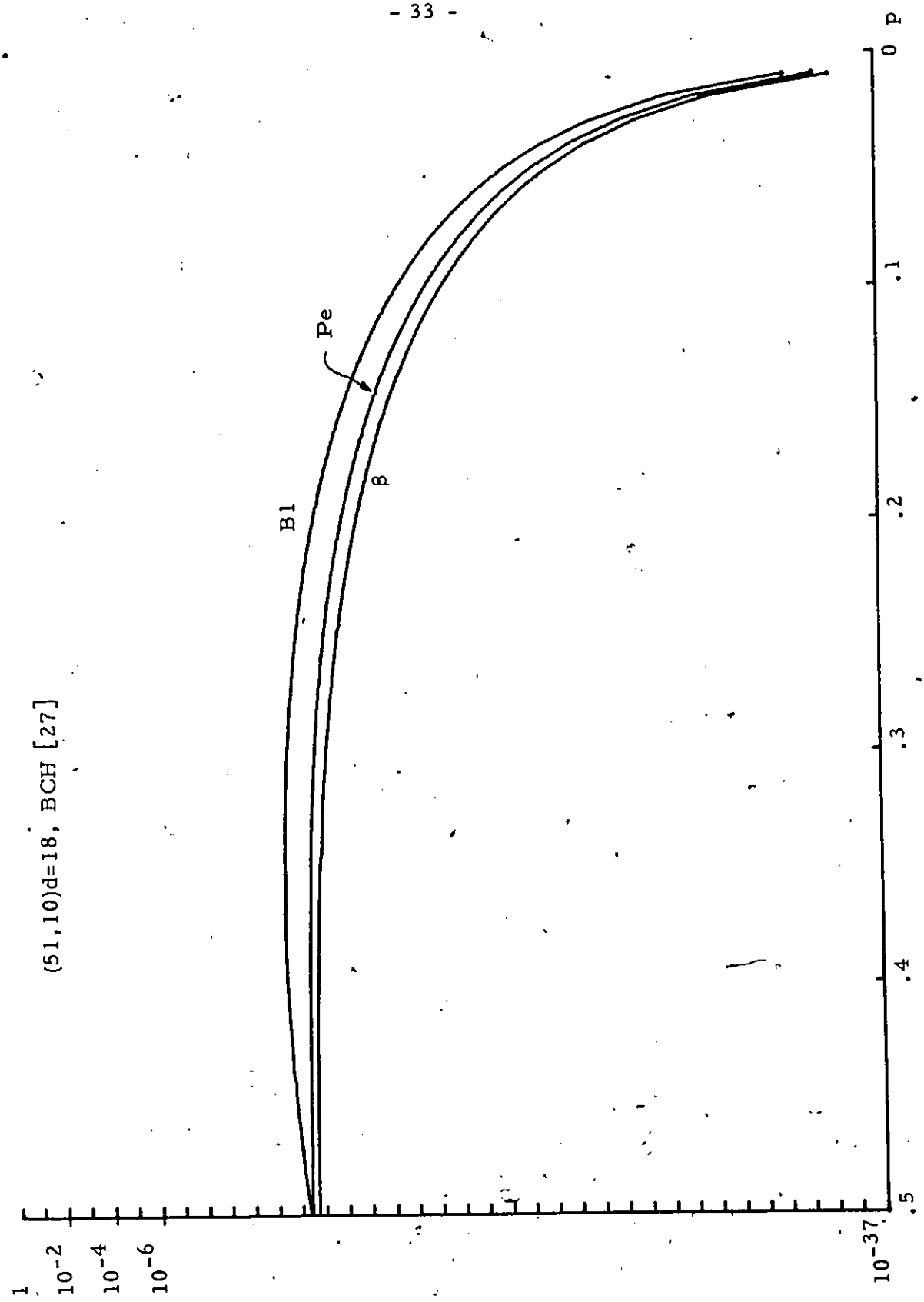

Figure 3.7

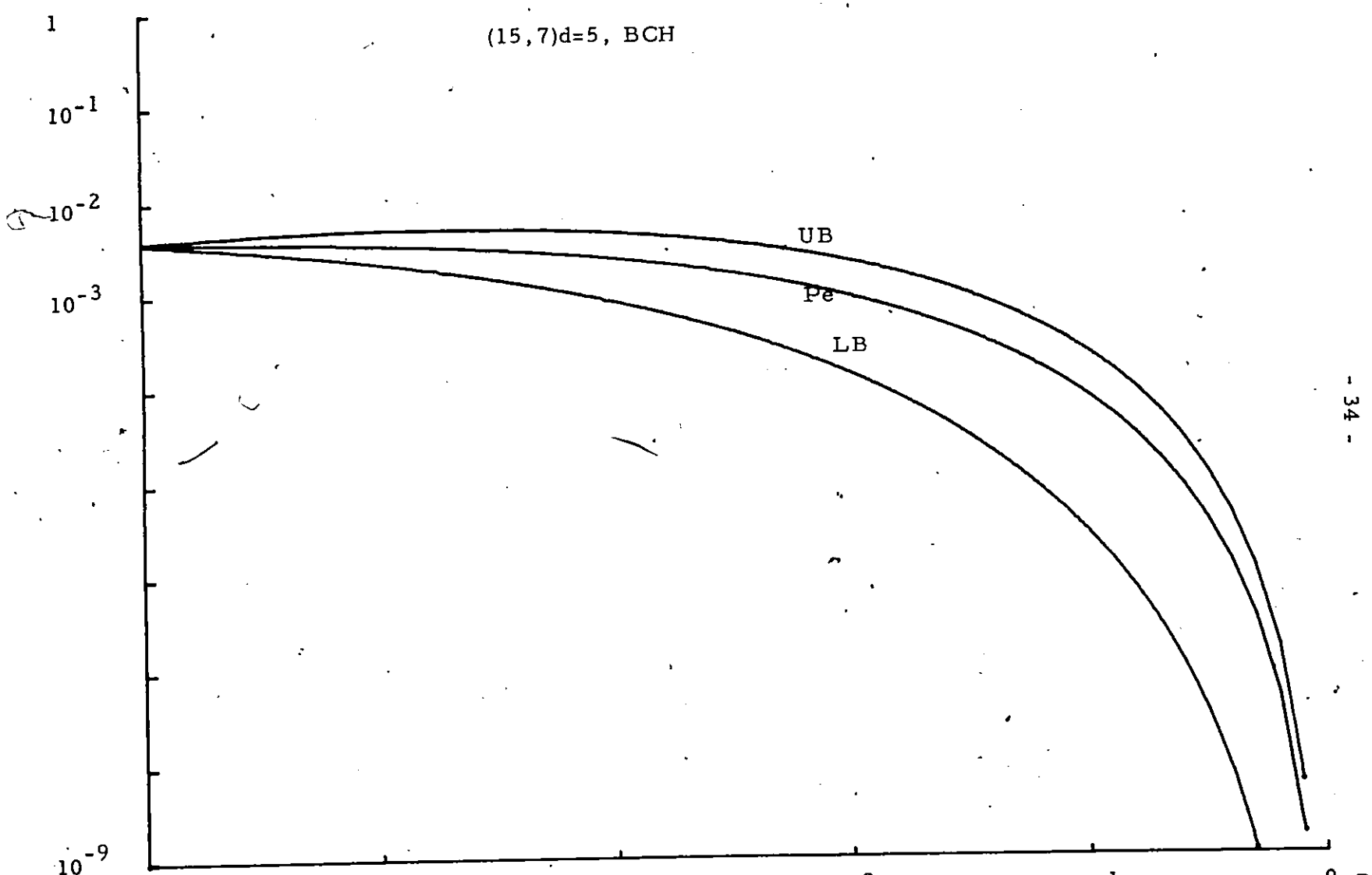

Figure 3.8

3.2 LOWER BOUNDS ON Pe

In cases when we have some knowledge of the weight distribution of the code, the problem of bounding Pe can be simplified by noticing that, for small values of p, Pe is strongly dominated by the first one or two terms of the summation in (3.1), i.e. Pe is greater than and approximately equal to

$$Pe' = A_d p^d (1-p)^{n-d} + A_{d+1} p^{d+1} (1-p)^{n-d-1} \qquad (3.5)$$

To evaluate Pe' we need to know A_d and A_{d+1}. We now quote a result that relates A_d and A_{d+1}, so that if one is known, the other can be calculated.

Definition [30] A group of permutations is said to be transitive if for any two symbols in a code word there exists a permutation that interchanges them, possibly rearranging other symbols at the same time. A code is called invariant under a transitive permutation, or simply transitive, if every transitive permutation carries every code word into another code word.

Consider a binary group code V, of block length n, and let V' be the extended code of length $n' = n+1$, formed by appending an even-parity bit to the code words of the code V.

Theorem 3.1 [36]

If the extended code V' is invariant under a transitive permutation group, then

$$A_{\omega-1} = \frac{\omega}{n+1-\omega} A_\omega, \quad \omega \text{ even} \qquad (3.6a)$$

and

$$A_{\omega-1} = \frac{\omega}{n+1} A'_\omega \qquad (3.6b)$$

where A_ω and A'_ω represent the number of code words of weight ω in the codes V and V' respectively.

It is known [30] that the Golay code, all quadratic residue codes, and all primitive BCH codes and primitive cyclic Reed-Muller codes have transitive extended codes, and therefore Theorem 3.1 applies for all of these codes.

Equation (3.6a) implies that if an even weight ω occurs in the code, the corresponsing odd weight $\omega-1$ also occurs. As an example, consider the (23, 12) d=7 Golay code. The weight distribution of this code is given in Table 3.1.

Table 3.1 Weight Distribution of the Golay Code [32]

Weight i	Number of Code Words of this Weight A_i
0	1
7	253
8	506
11	1288
12	1288
15	506
16	253
23	1

We notice from this table that there are no words of weight 9 or 13. But the weights 10 and 14 are also absent, which agrees with equation (3.6a) .

Now suppose that the relation given by (3.6a) is true for any ω:

$$\frac{A_{\omega-1}}{A_\omega} \approx \frac{\omega}{n+1-\omega}$$

Using this rough estimate of the weight distribution we write

$$Pe \approx A_d p^d (1-p)^{n-d} \left[1 + \frac{n-d}{d+1} \frac{p}{(1-p)} + \frac{(n-d)}{(d+1)} \frac{(n-d-1)}{(d+2)} \left(\frac{p}{1-p}\right)^2 + \right.$$

$$\left. + \ldots \right] \qquad (3.7)$$

Under this approximation, if the term $\frac{(n-d)}{(d+1)} \frac{(n-d-1)}{(d+2)} \left(\frac{p}{1-p}\right)^2 << 1$ then this and the successive terms are negligible. Therefore (3.7) reduces to equation (3.5) which can be rewritten as

$$Pe > Pe' = A_d p^d (1-p)^{n-d} \left[1 + \frac{n-d}{d+1} \frac{p}{1-p} \right] \qquad (3.8)$$

For small values of p, (3.8) is a tight lower bound on Pe as illustrated by Examples 3.2 and 3.3 and Figures 3.9 and 3.10.

For the sake of convenience, we present without proof the following well known theorems [31]

Theorem 3.2 Let V be a single-error correcting BCH code of length $n = 2^m - 1$. Then

$$A_d = A_3 = \frac{n(n-1)}{3!}$$

Theorem 3.3 Let V be a double-error correcting code of length $2^m - 1$, m even. Then

$$A_d = A_5 = \frac{n(n-3)^2}{5!}$$

Example 3.2

Consider the (15,7) d = 5 BCH code and let p = .01.

Then from Theorem 3.3, $A_5 = \frac{15(12)^2}{120} = 18$

from (3.6a), $A_6 = \frac{10}{6} \cdot 18 = 30$

and $Pe' = 18 (.01)^5 (.99)^{10} + 30 (.01)^6 (.99)^9 = 1.655293252 \times 10^{-9}$

The exact value of Pe is given by

$$Pe = \sum_{i=5}^{10} A_i (.01)^i (.99)^{15-i} + (.01)^{15} = 1.655433091 \times 10^{-9}.$$

The third term in the expansion of Pe is

$$A_7 p^7 (1-p)^8 = 15 (.01)^7 (.99)^8 = 1.384117042 \times 10^{-13}.$$

The contribution to Pe of this and subsequent terms is negligible.

Example 3.3

Consider the (23, 12) d = 7 Golay code and let p =.01.

From Table 3.1, $A_7 = 253$, $A_8 = 506$ and

$$Pe = 253(.01)^7 (.99)^{16} + 506 (.01)^8 (.99)^{15}$$

$$= 2.197707114 \times 10^{-12}$$

Pe is given by

$$Pe = 253 (.01)^7 (.99)^{16} + 506(.01)^8 (.99)^{15} + 1288 (.01)^{11}(.99)^{12} +$$

$$+ 1288 (.01)^{12} (.99)^{11} + 506 (0.1)^{15}(.99)^8 + 253(.01)^{16}(.99)^7 + (.01)^{23}$$

$$= 2.197707229 \times 10^{-12}$$

The third term of Pe, $1288 (.01)^{11} (.99)^{12} = 1.141663715 \times 10^{-19}$ is again negligible, as are all subsequent terms. ———

A similar reasoning to that used to derive UB, (eq. (3.4)), can be used to form a lower bound on Pe when it is known that the code contains the word of all ones but we have no knowledge of A_d.

$$Pe \geq LB = p^{\frac{n-1}{2}}(1-p)^{\frac{n+1}{2}}(2^{k-1}-1) + p^{n-d}(1-p)^{d}(2^{k-1}-1) + p^{n} \quad (3.9)$$

In this equation we have divided the expression for Pe (eq. (3.1)) in half and taken the smallest term of the binomial expansion times half of the code words as a lower bound for each half or Pe. Equation (3.9) is plotted for the (15,7) d = 5 BCH code in Fig. 3.8.

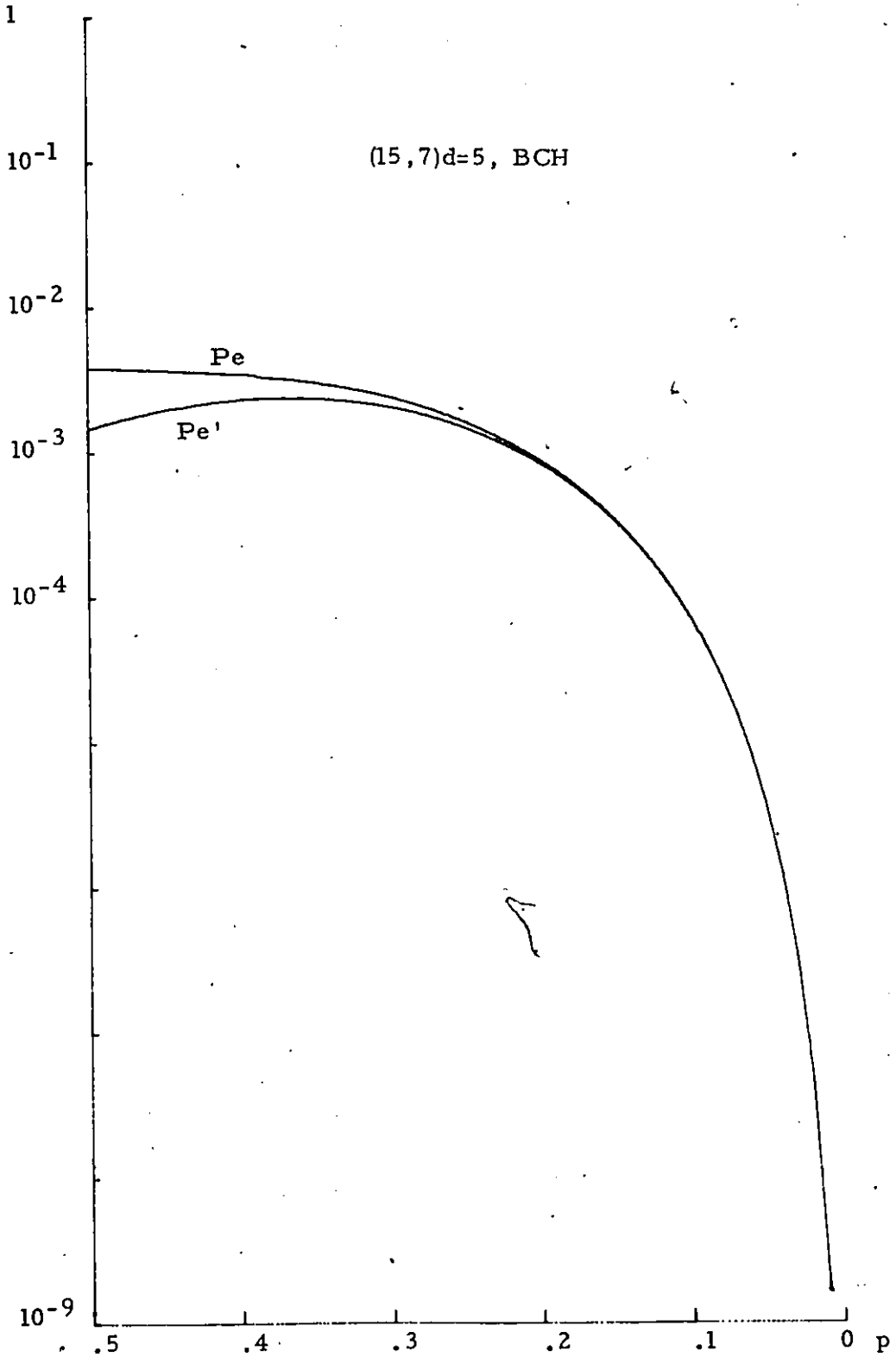

Figure 3.9

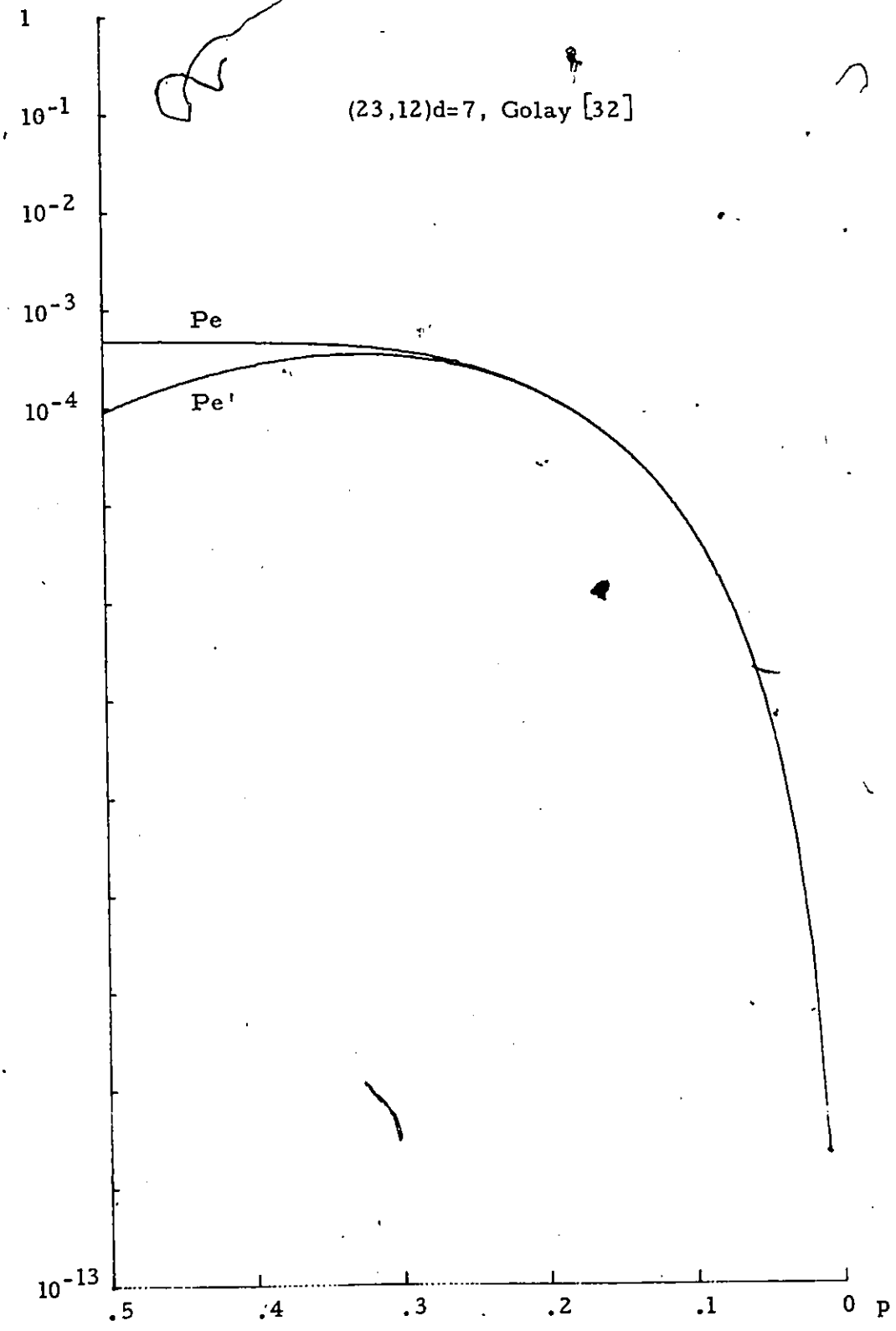

Figure 3.10

3.3 AN APPROXIMATION FOR Pe

We will now show that it is possible to approximate Pe by using the random coding argument. No knowledge of the weight distribution of the code is required.

The approximation is derived as follows. Consider forming an (n,k) code by selecting at random and, with replacement, 2^k n-tuples from the entire set of 2^n n-tuples. In the set of 2^n n-tuples there are $\binom{n}{i}$ n-tuples of weight i, therefore in the 2^k chosen n-tuples there will be on the average $\frac{\binom{n}{i}}{2^n} 2^k = \binom{n}{i} 2^{k-n}$ n-tuples of weight i.

The fact that an algebraic structure is imposed on codes formed algebraically causes deviations from the number expected due to the random coding argument. However the effect of these deviations should be averaged out when a large number of different weights is considered. This has been verified by a computer analysis of a number of codes.

If in equation (3.1) we substitute

$$\binom{n}{i} 2^{-(n-k)} \quad \text{for} \quad A_i \quad \text{if} \quad A_i \neq 0,$$

we get an approximation for Pe which we will call β :

$$Pe \approx \beta = \frac{1}{2^{n-k}} \left[\binom{n}{d} p^d (1-p)^{n-d} + \binom{n}{d+1} p^{d+1} (1-p)^{n-d-1} + \ldots + \binom{n}{n-1} p^{n-1} (1-p) \right] + p^n .$$

$$= \frac{1}{2^{n-k}} \sum_{i=d}^{n-1} \binom{n}{i} p^i (1-p)^{n-i} + p^n . \qquad (3.10)$$

Before using this approximation we have to gather all information possible about the weights present in the code. The following results are useful in this respect.

1) Let V be an (n,k) cyclic code generated by a $g(x)$ which is relatively prime with $(1+x)$, (i.e. $(1+x)$ is not a factor of $g(x)$). Then the n-tuple of all 1's is a codeword. From this we know that $A_i = 0$ for $0 < i < d$ and $n-d < i < n$.

2) Let V be an (n,k) cyclic code generated by $g(x)$. If $(1+x)$ is a factor of $g(x)$, then the code is even-weighted, i.e. $A_j = 0$, j odd.

This can be checked by looking at the roots of $g(x)$ [28]. If 1 is not a root of $g(x)$, then $(1+x)$ is not a factor and the word of all ones is present in the code. This implies that there are no codewords of weight ω, for $0 < \omega < d$, and $n-d < \omega < n$. The words of the code are then picked not from 2^n but from $2^n - 2\sum_{j=1}^{d-1}\binom{n}{j}$ and the approximation (3.10) becomes

$$Pe \approx \beta = \frac{2^k}{2^n - 2\sum_{j=1}^{d-1}\binom{n}{j}} \sum_{i=d}^{n-d}\binom{n}{i} p^i (1-p)^{n-i} + p^n. \quad (3.11)$$

If 1 is a root of $g(x)$, then $(1+x)$ is a factor of $g(x)$ and only the even weights are present in the code. The words are picked not from 2^n but from $2^{n-1} - \sum_{j=1}^{\frac{d-1}{2}}\binom{n}{2j}$ and the approximation (3.10) becomes

$$Pe \approx \beta = \frac{2^k}{2^{n-1} - \sum_{j=1}^{d-1/2}\binom{n}{2j}} \sum^{\frac{n-d-1}{2}}\binom{n}{d+2i} p^{d+2i} (1-p)^{n-d-2i}. \quad (3.12)$$

However, with respect to (3.11) and (3.12), if instead of using

$$\frac{2^k}{2^n - 2\sum_{j=1}^{d-1}\binom{n}{j}} \quad \text{and} \quad \frac{2^k}{2^{n-1} - \sum_{j=1}^{d-1/2}\binom{n}{2j}} \quad \text{we use} \quad \frac{1}{2^{n-k}},$$

we get a simpler expression for β, without much affecting its final value.

Then the forms used for the approximations will be

$$\beta = \frac{1}{2^{n-k}} \sum_{i=d}^{n-d} \binom{n}{i} p^i (1-p)^{n-i} + p^n \qquad (3.13)$$

for codes with the word of all ones, and

$$\beta = \frac{1}{2^{n-k}} \sum_{i=o}^{\frac{n-d-1}{2}} \binom{n}{d+2i} p^{d+2i} (1-p)^{n-d-2i} \qquad (3.14)$$

for even-weighted codes.

We now present an example illustrating the application of equations (3.13) and (3.14) to particular codes.

Example 3.4

Consider the (21, 12) d = 5 BCH code. This code is generated by $g(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^9$ [28].

Because 1 is not a root of this polynomial, the code must have weights restricted to 0, 5, 6, 7, . . . , 15, 16, 21. Then β is given from (3.13) by

$$\beta = \frac{1}{2^9} \sum_{i=5}^{16} \binom{21}{i} p^i (1-p)^{21-i} + p^{21}.$$

The (21, 11) d = 6 BCH code is generated by

$$g'(x) = g(x)\ (1+x) = 1 + x^3 + x^4 + x^6 + x^8 + x^{10} \quad [28] .$$

Since (1+x) is a factor of g(x) we know that the code contains even-weighted words only.

From (3.14) β is given by

$$\beta = \frac{1}{2^{10}} \sum_{i=o}^{7} \binom{21}{6+2i} p^{6+2i} (1-p)^{15-2i} .$$

In Figures 3.1 to 3.7 we have plotted B1, Pe and β for various codes, and in Figures 3.11 to 3.26 we have plotted Pe and β for other codes. We see that β is a good approximation of Pe. For all the codes considered, β is consistently less than Pe by a small amount ; the ratio $\frac{Pe}{\beta}$ is much less than $\frac{B1}{Pe}$.

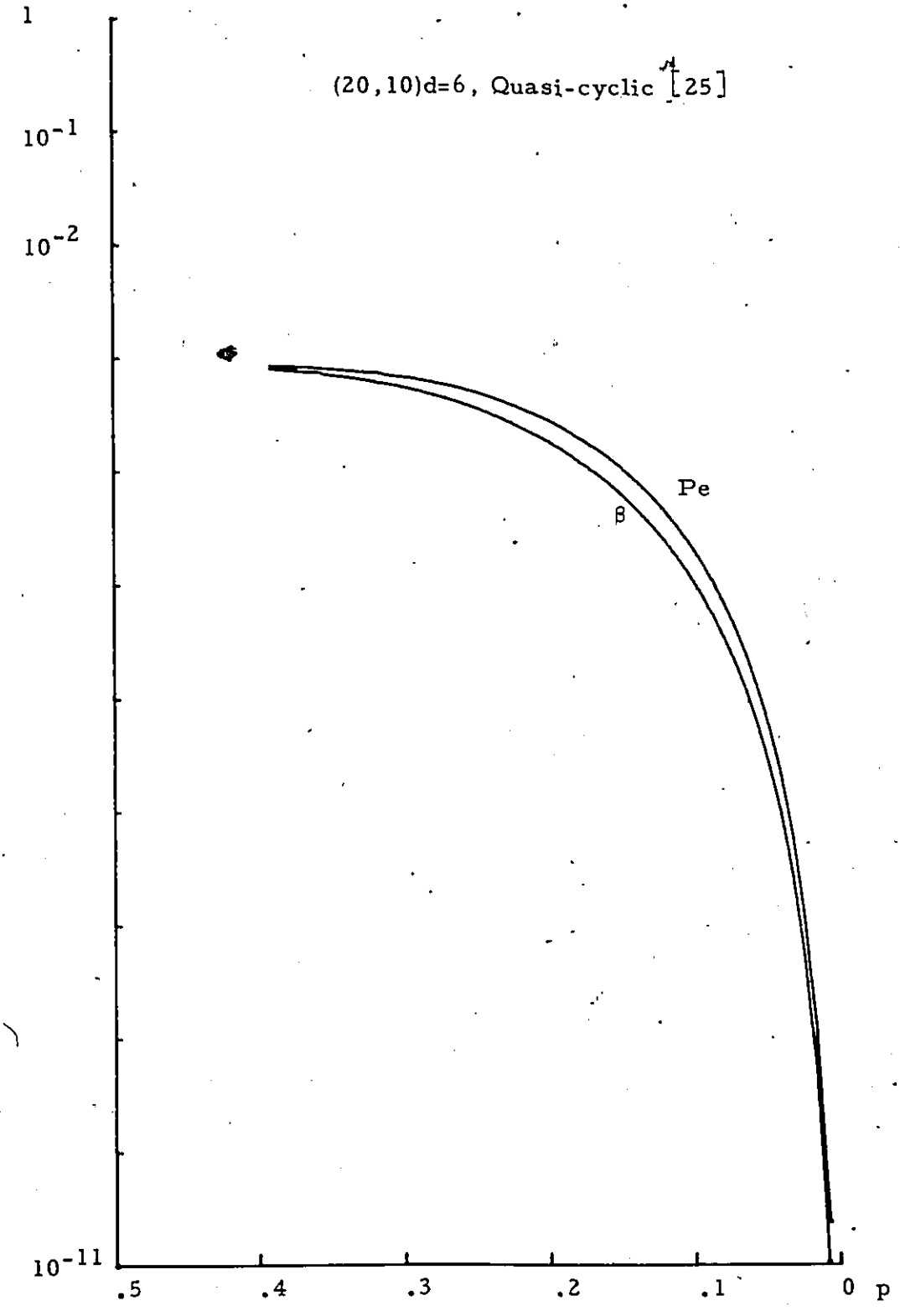

Figure 3.11

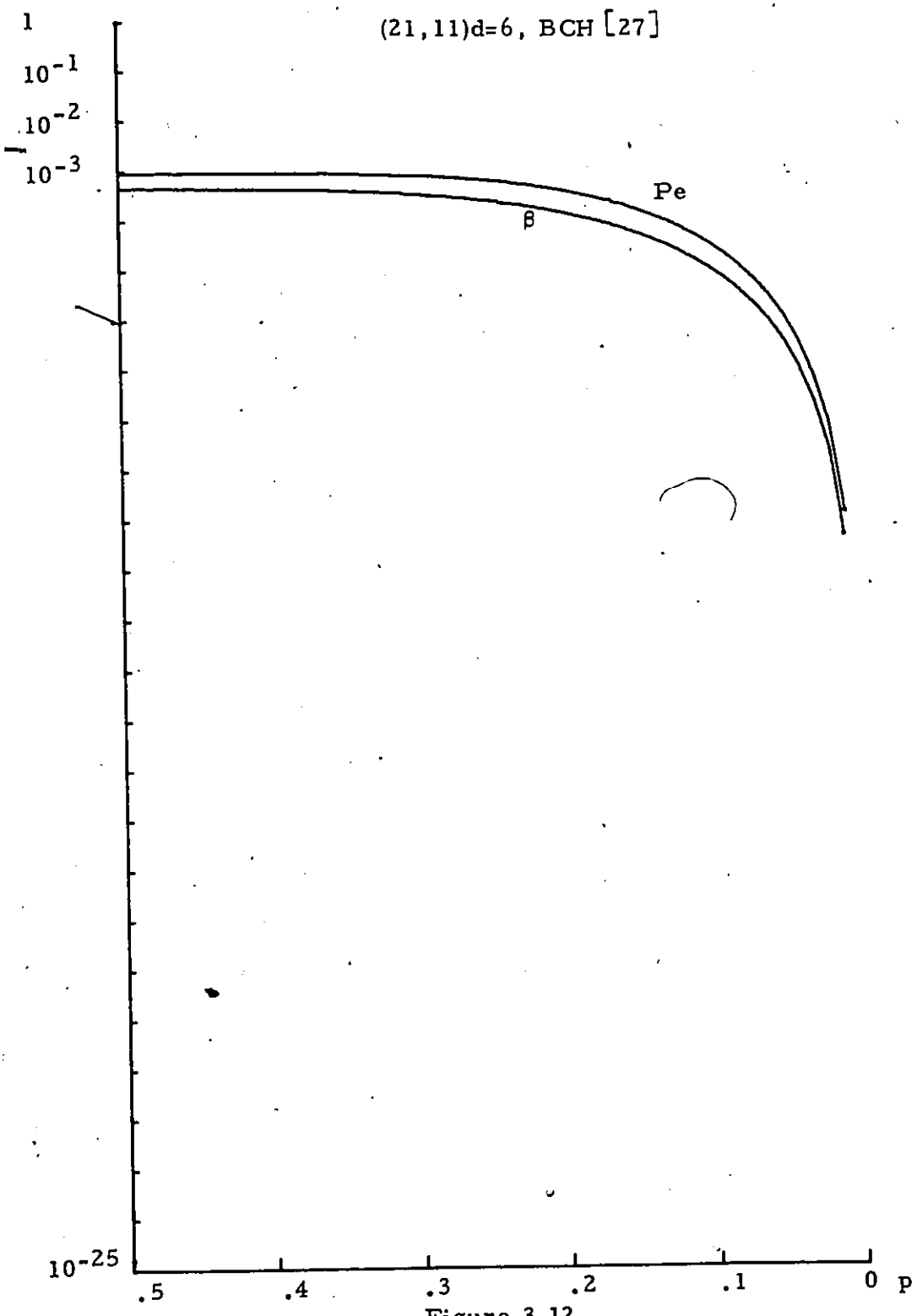

Figure 3.12

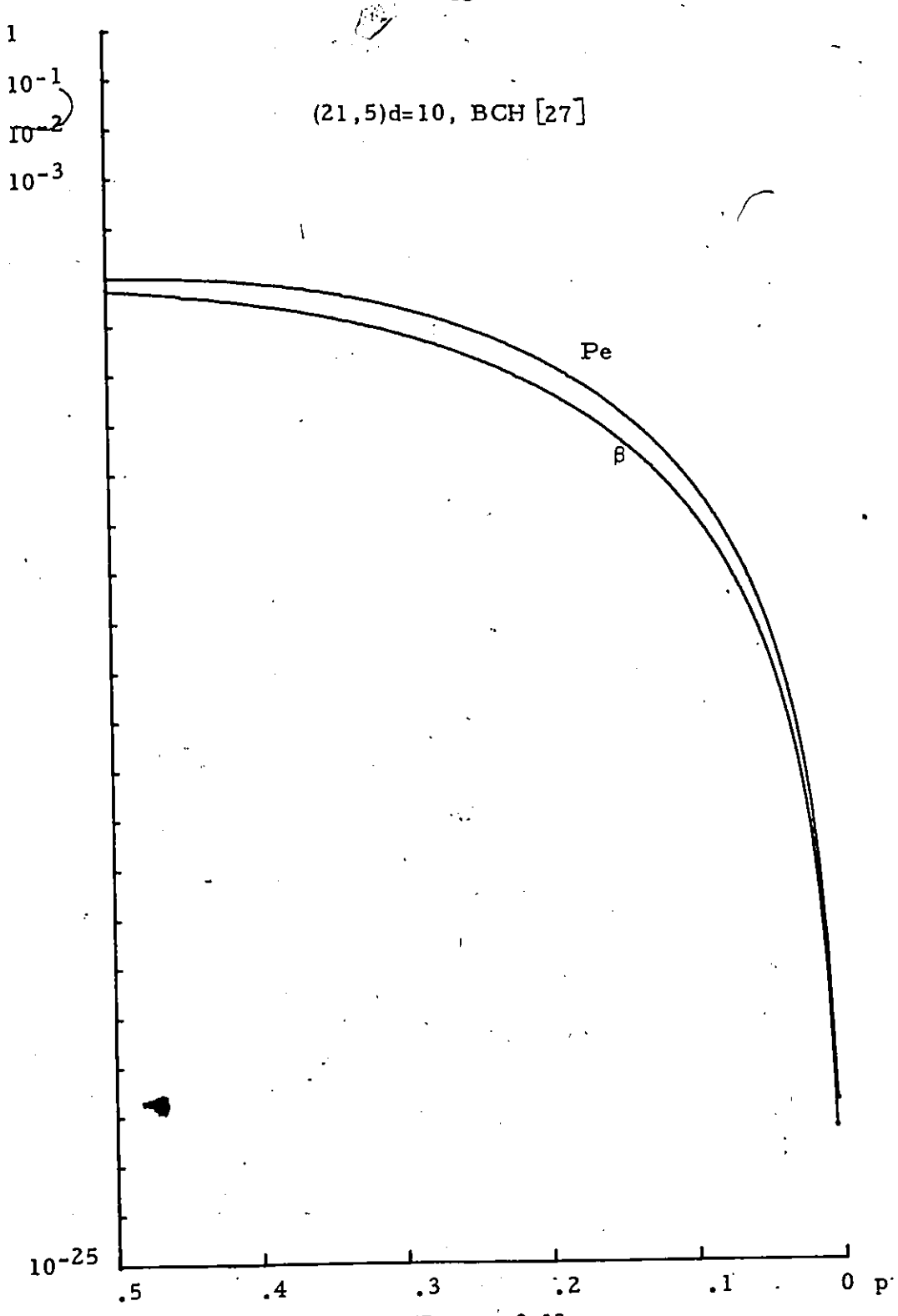

Figure 3.13

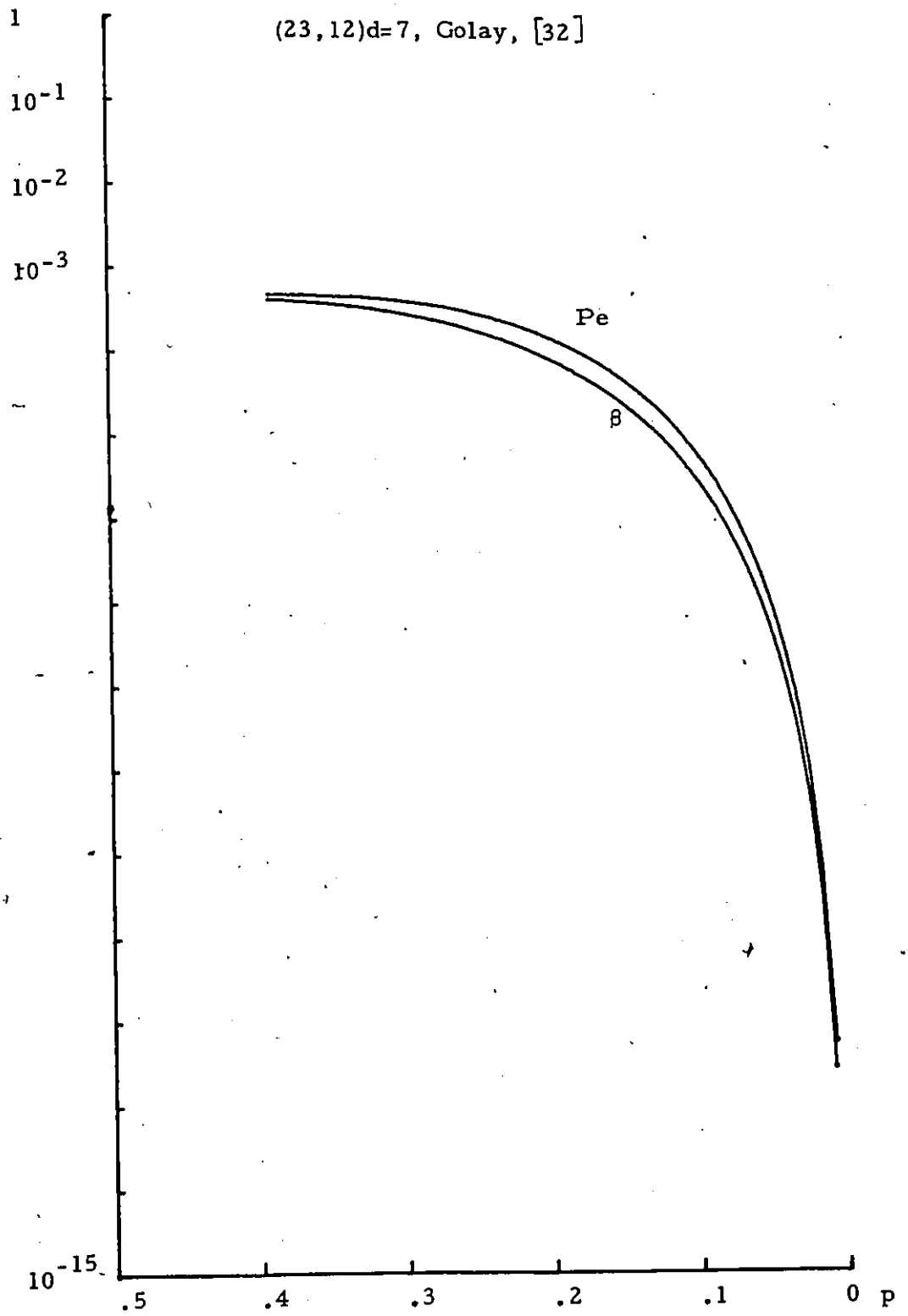

Figure 3.14

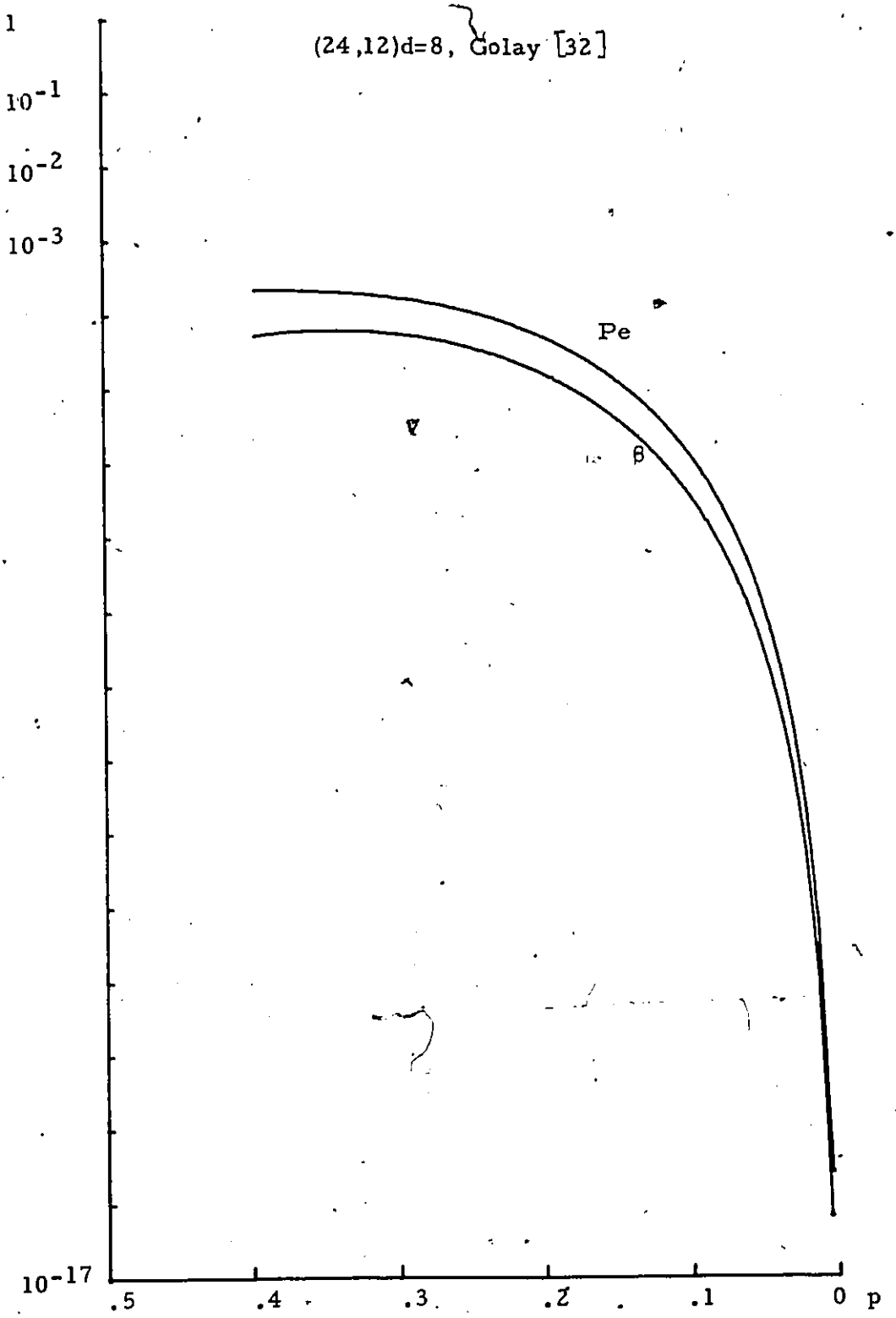

Figure 3.15

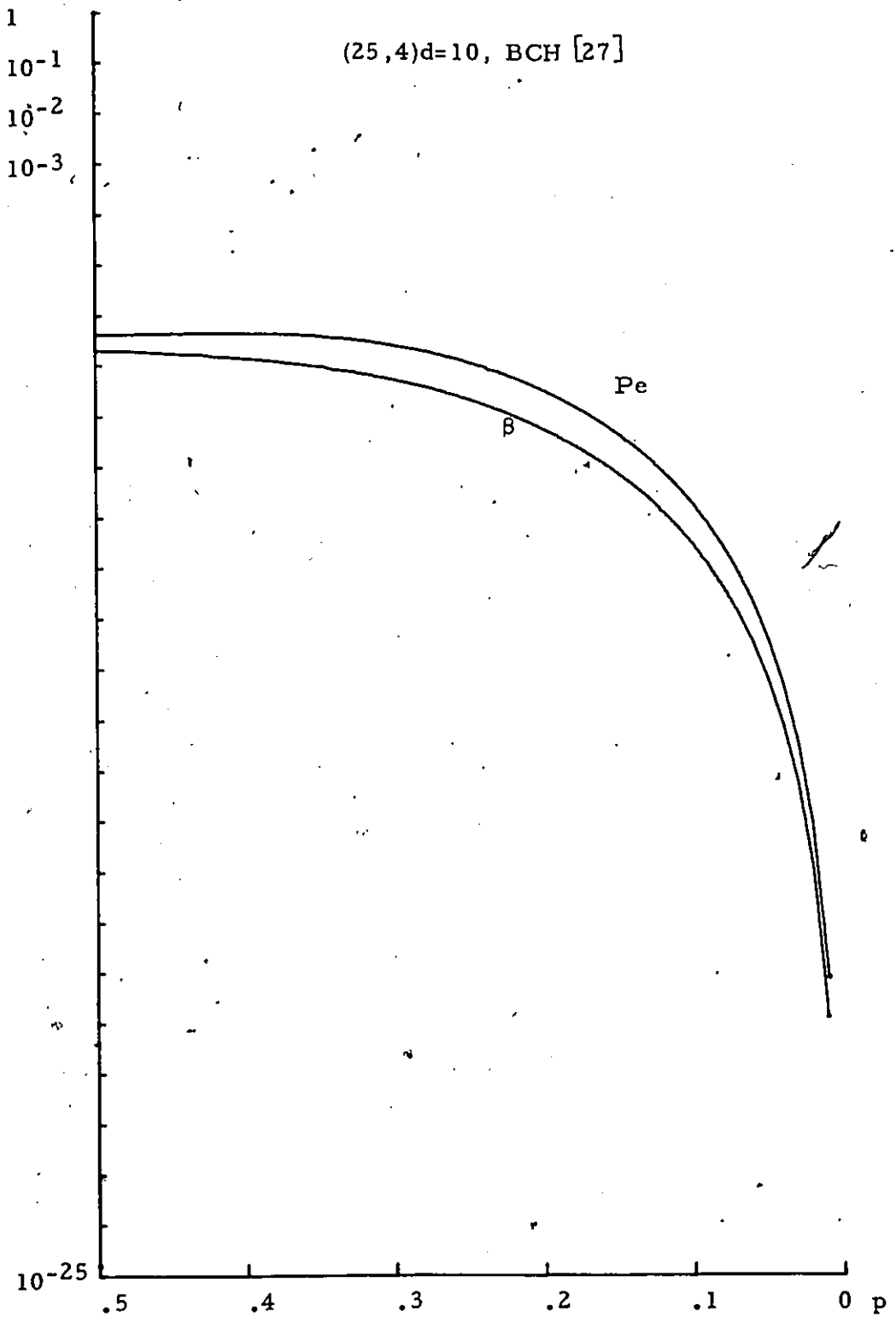

Figure 3.16

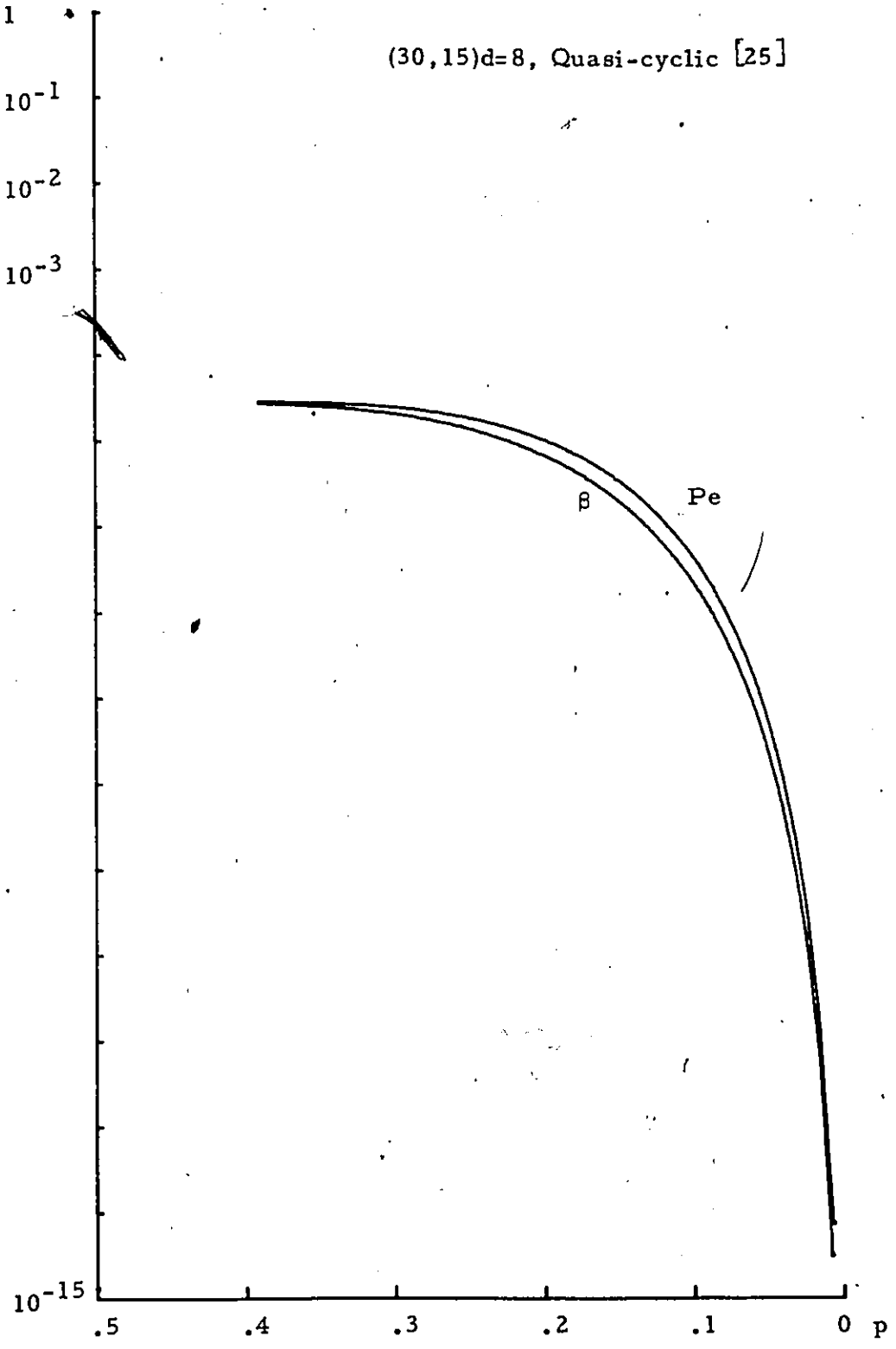

Figure 3.17

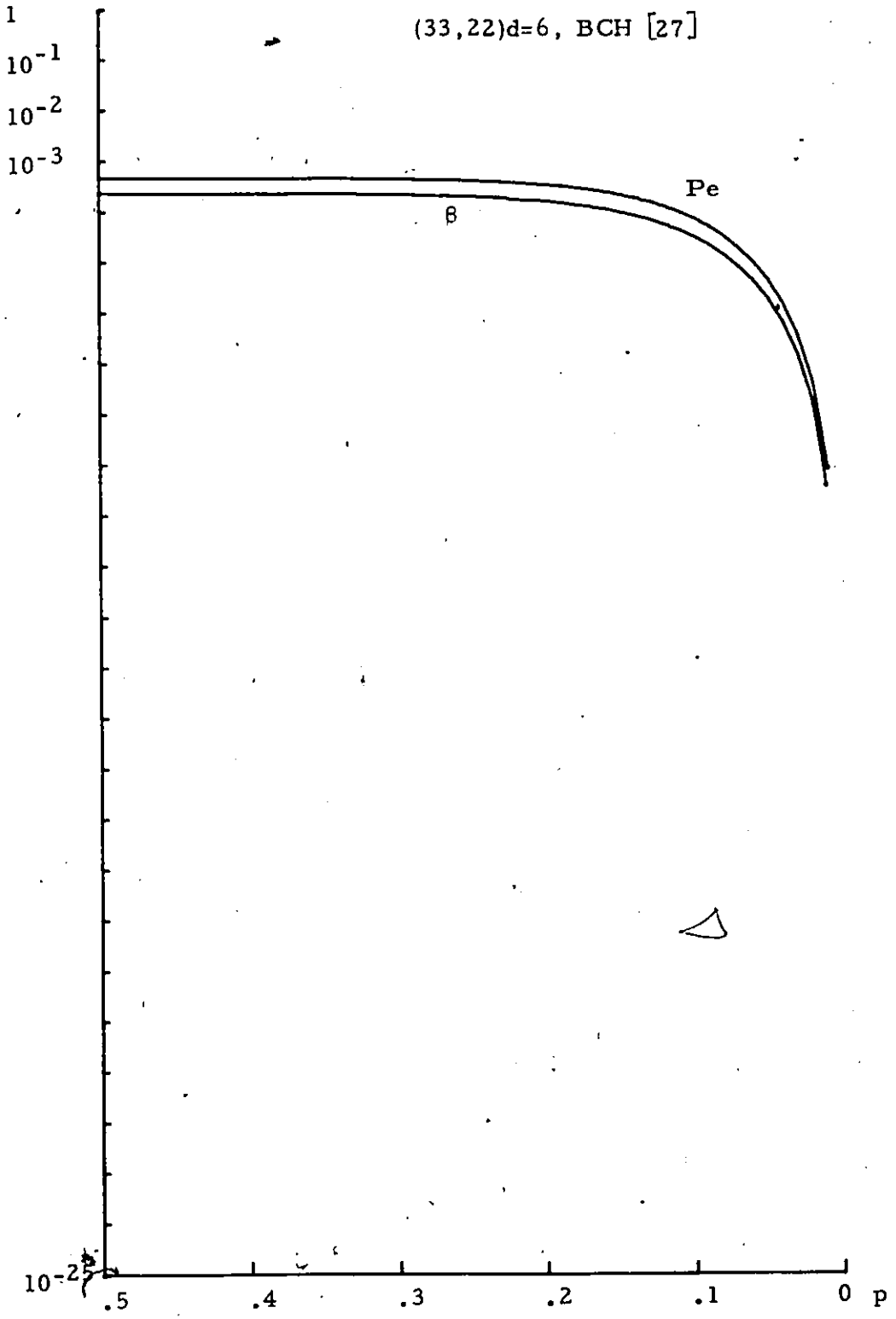

Figure 3.18

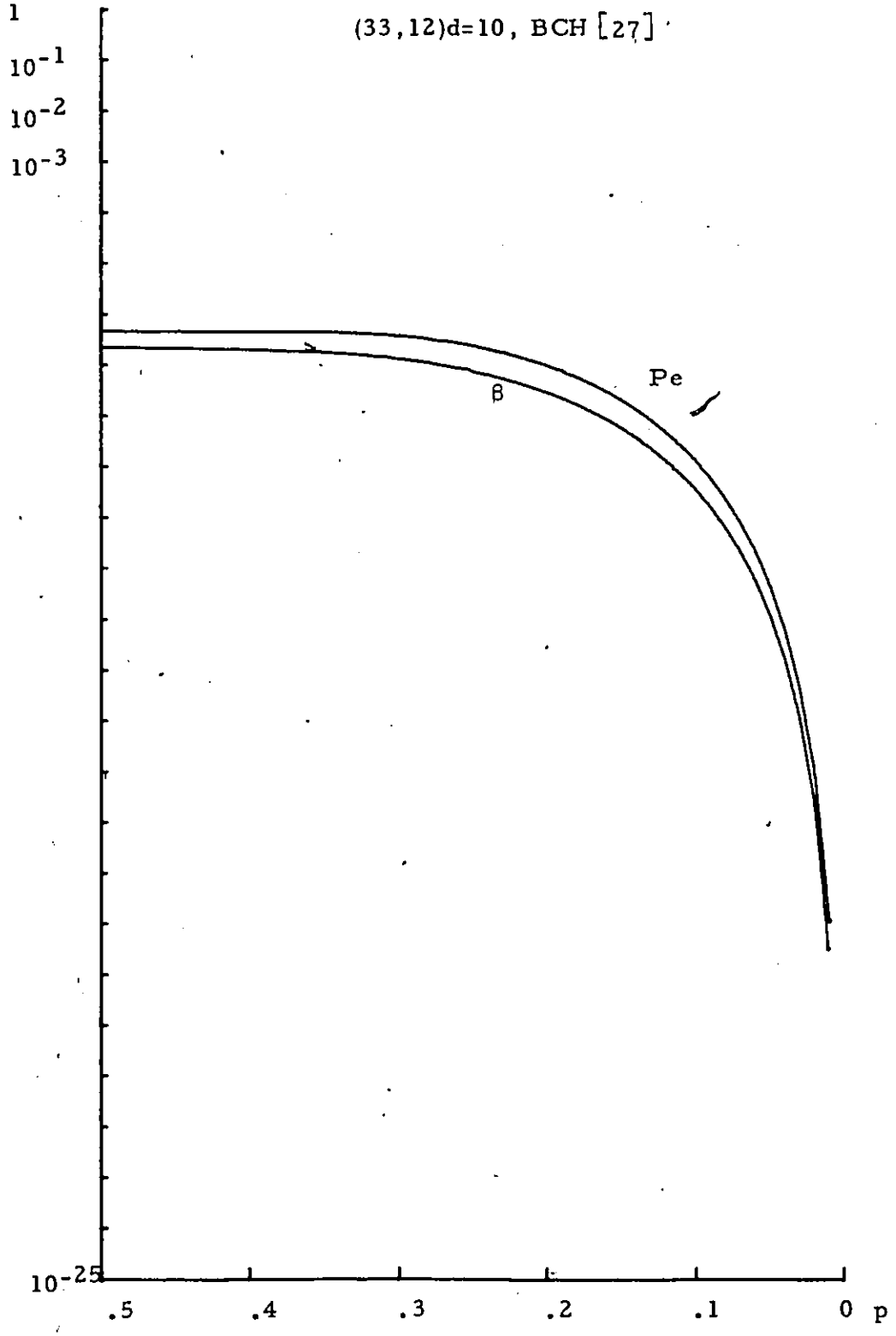

Figure 3.19

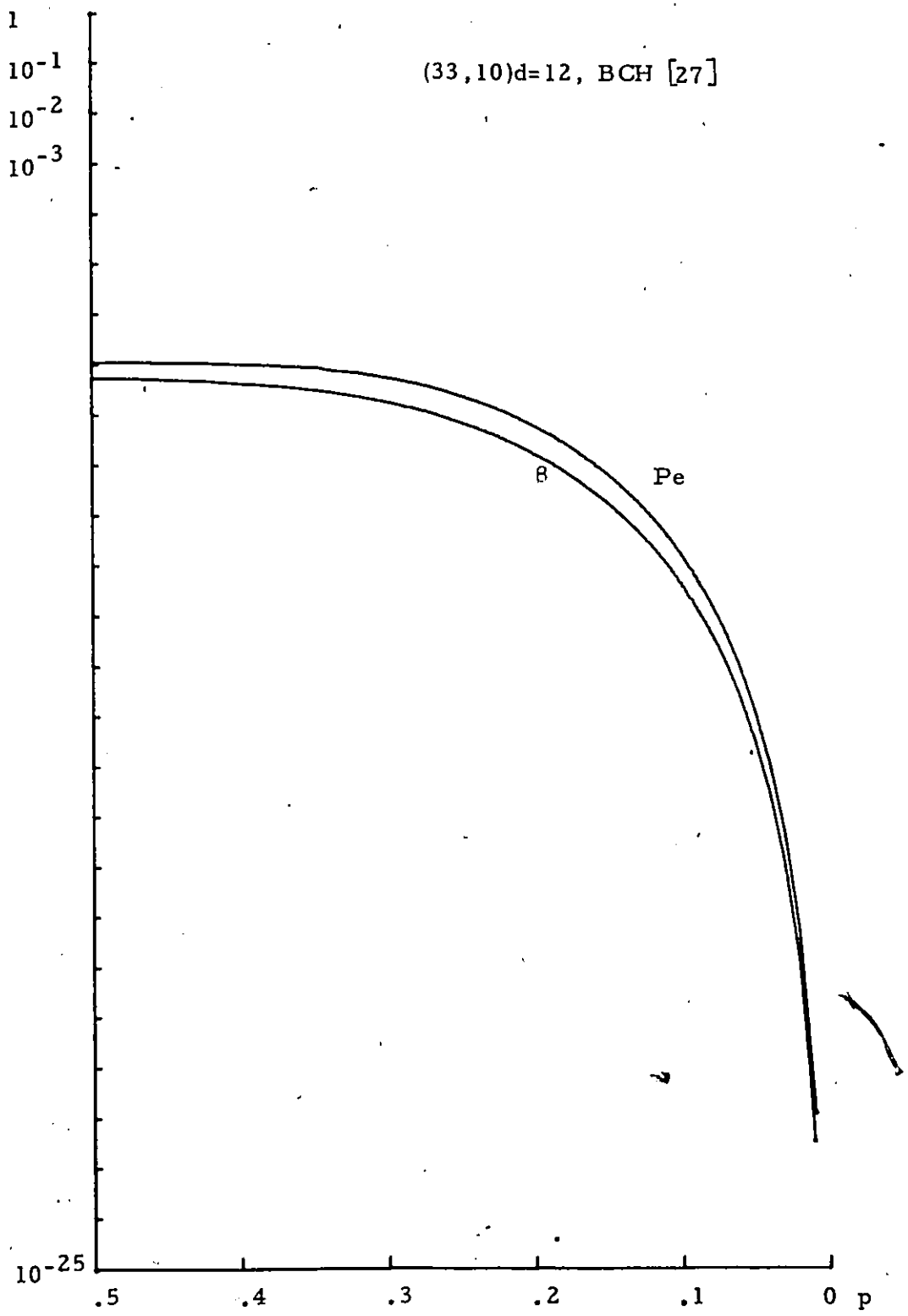

Figure 3.20

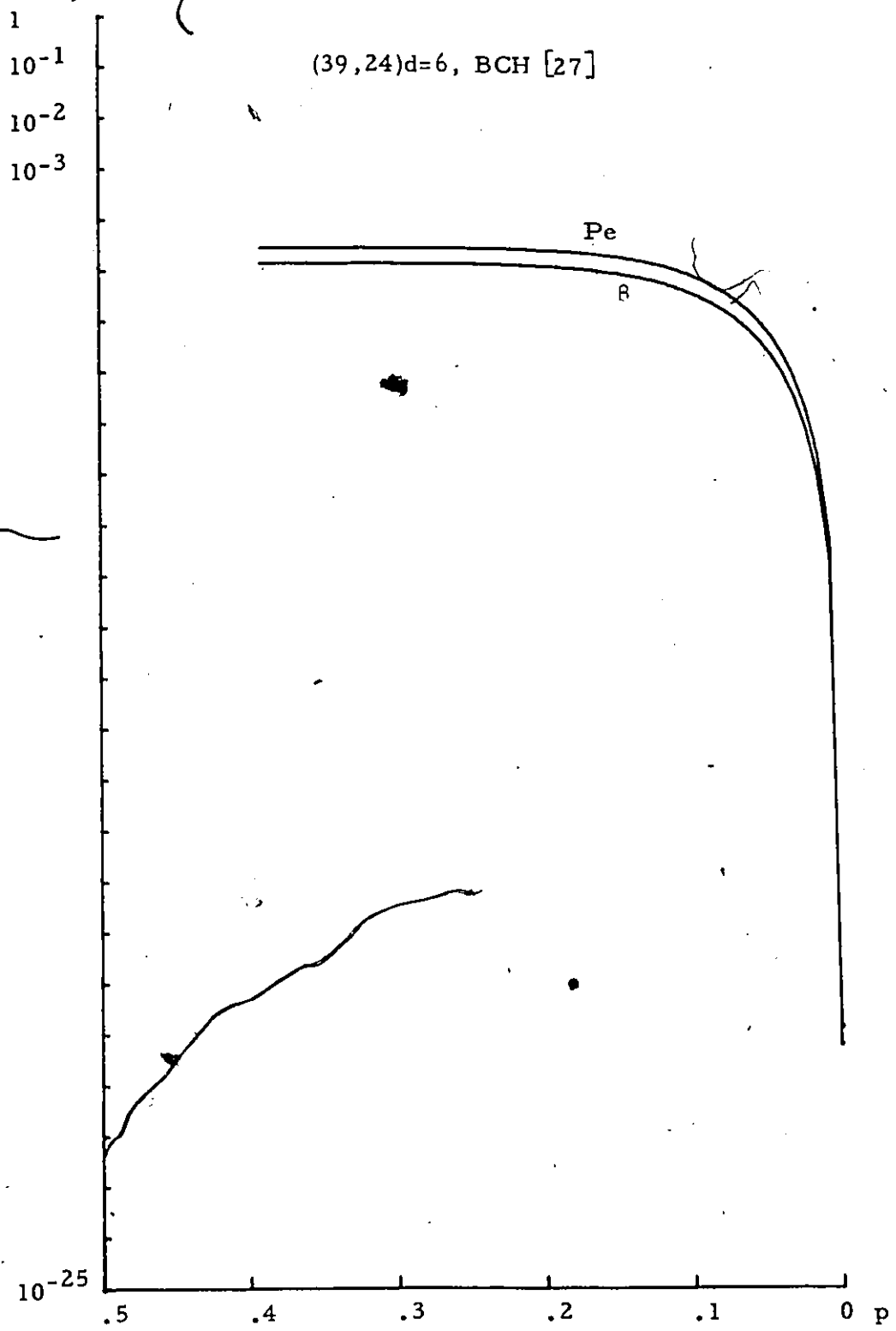

Figure 3.21

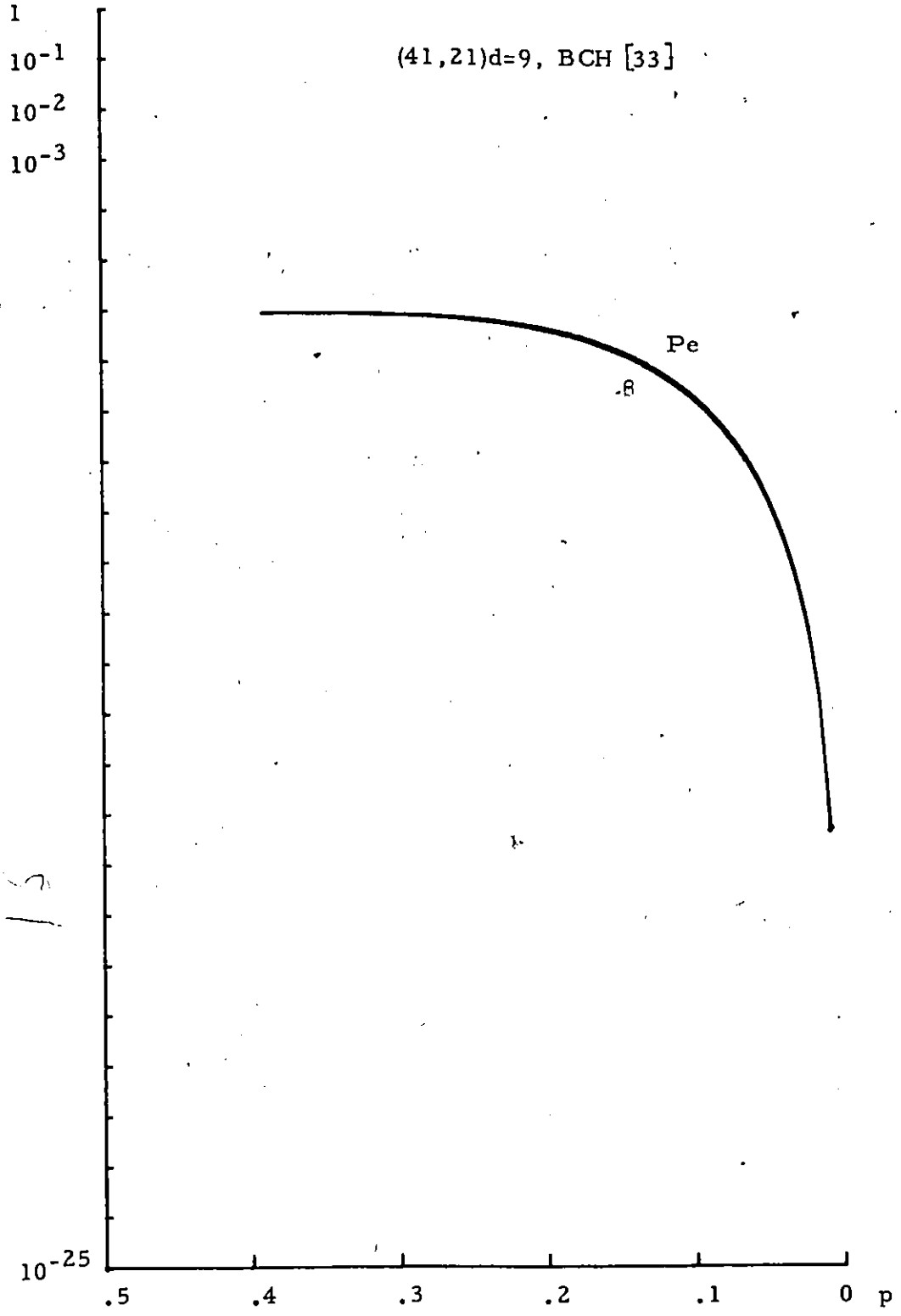

Figure 3.22

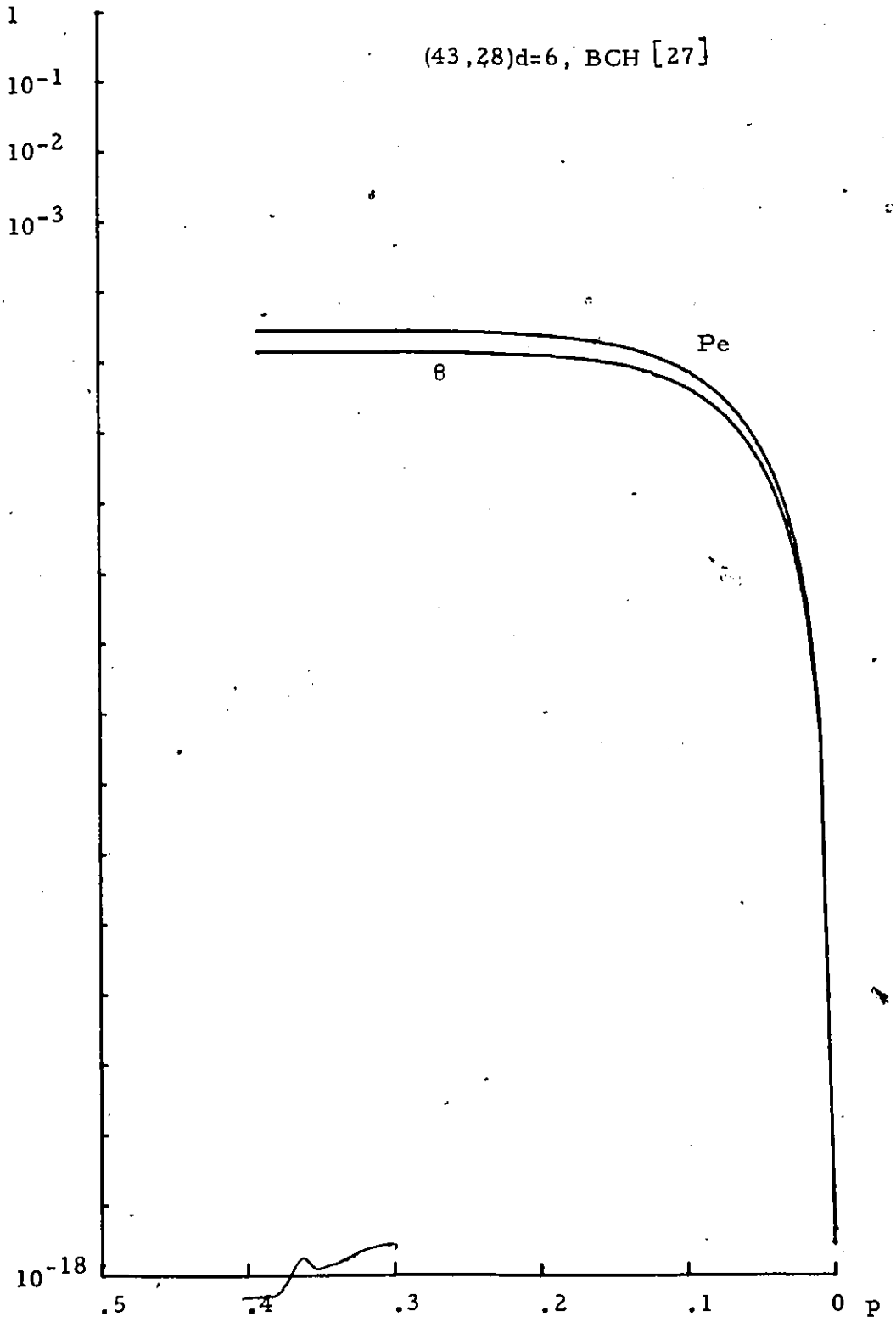

Figure 3.23

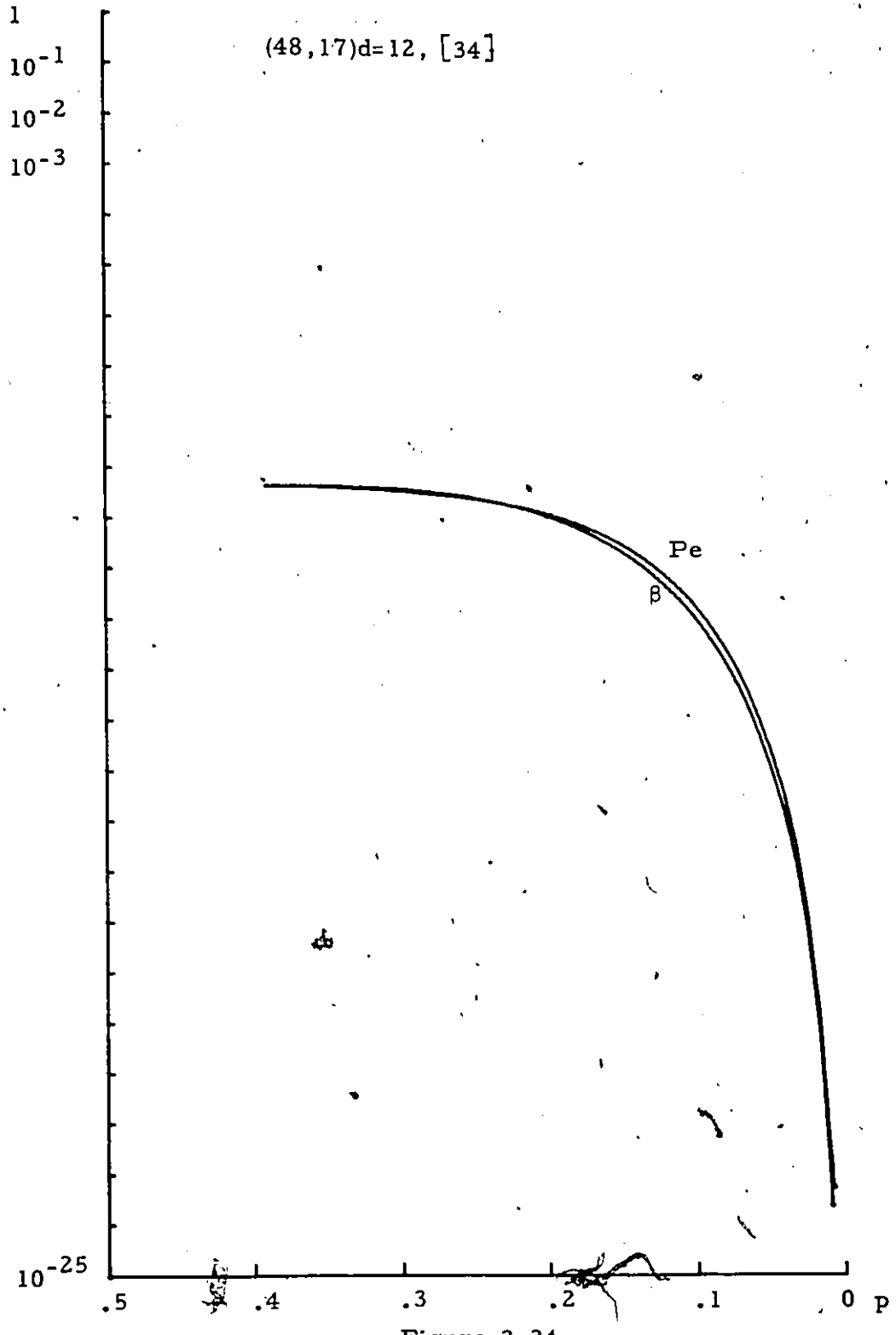

Figure 3.24

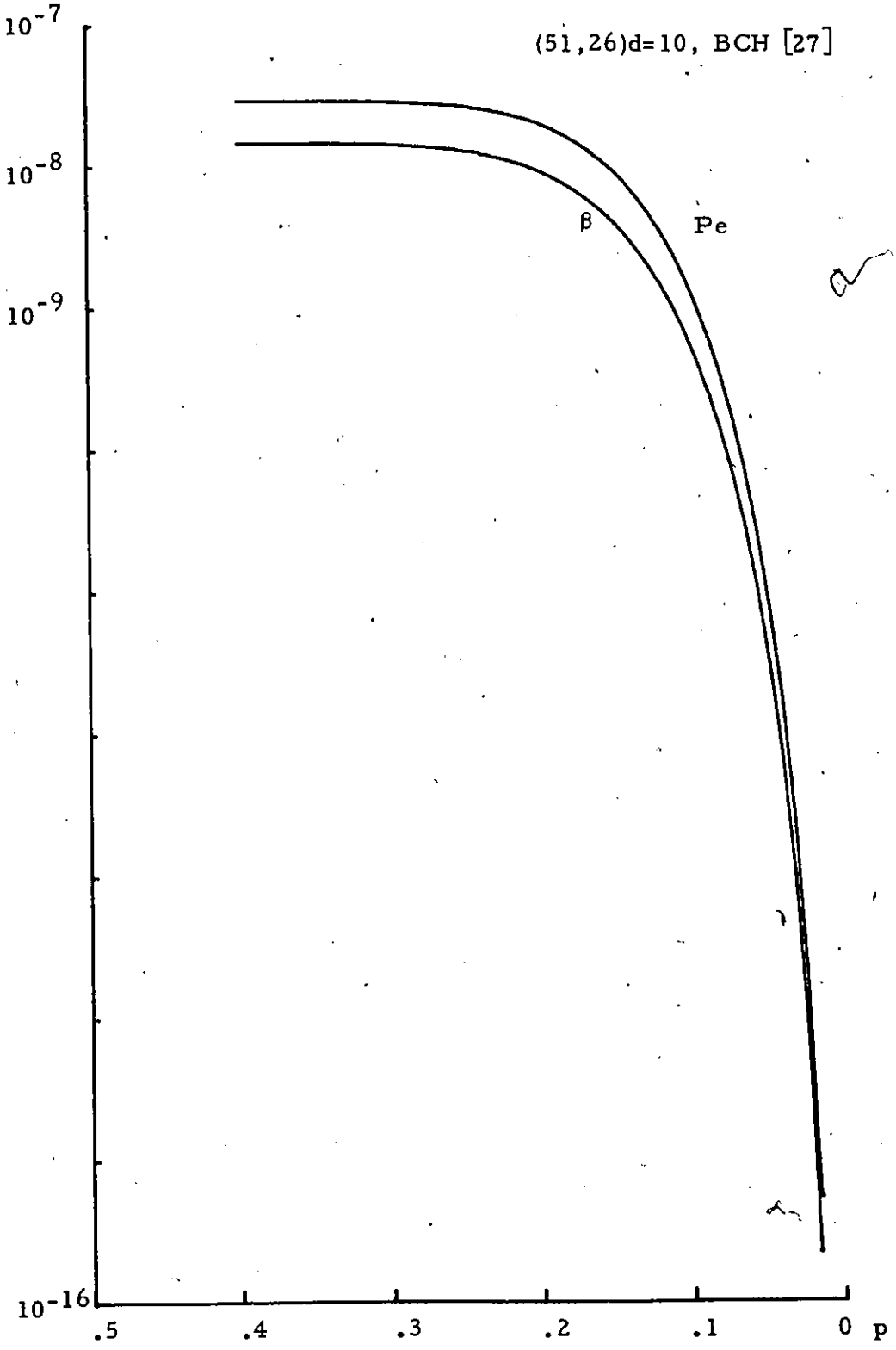

Figure 3.25

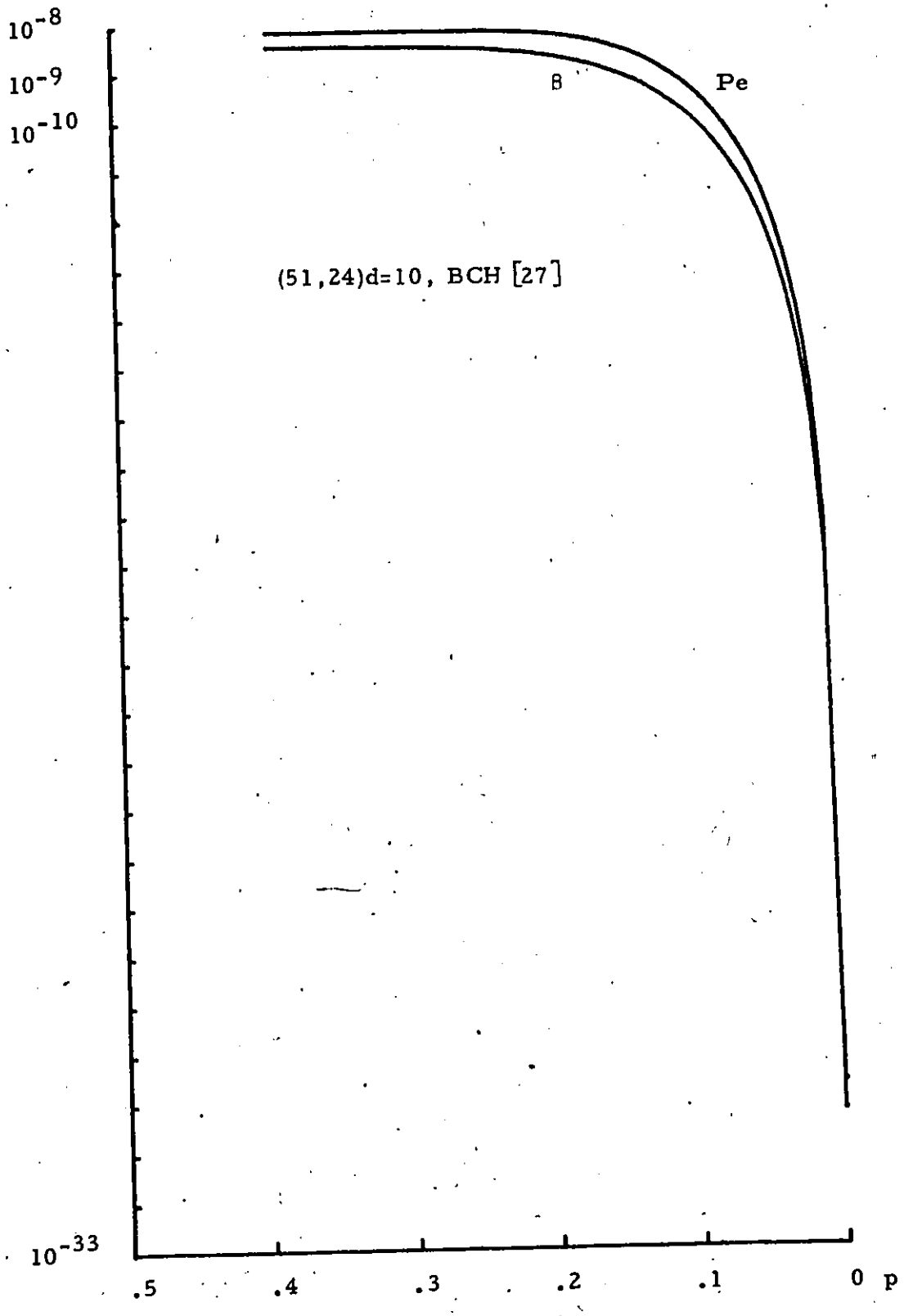

Figure 3.26

3.4 ON THE USE OF EVEN-WEIGHTED CODES FOR ERROR DETECTION.

Let us choose an $(n,k-1)$ code, V_2, which is the even-weighted subset of an (n,k) code, V_1. The probabilities Pe_1 and Pe_2 of undetected errors for V_1 and V_2 respectively, when used in a binary symmetric channel with crossover probability p are given by

$$Pe_1 = \sum_{i=d}^{n} A_i \, p^i (1-p)^{n-i}, \tag{3.15}$$

and if V_1 has n and d odd,

$$Pe_2 = \sum_{j=d+1}^{n-1} A_j \, p^j (1-p)^{n-j}, \quad j \text{ even}. \tag{3.16}$$

From these equations we see that

$$Pe_1 = Pe_2 + \sum_{z=d}^{n} A_z \, p^z (1-p)^{n-z}, \quad z \text{ odd}.$$

or $Pe_1 > Pe_2$.

It is clear then that the even-weighted subset of a code gives a lower Pe than the parent code. In this section we will estimate the ratio $\frac{Pe_1}{Pe_2}$ which is a measure of the improvement obtained by using the even-weighted subset of a code V_1 with n and d odd.

Let the extended code formed from V_1 by adding an even parity bit to each codeword be V_1'.

Theorem 3.4

If V_1' is invariant under a transitive permutation group [36], and $p \leq \frac{d+1}{n+1}$, then

$$Pe_1 > 2\,Pe_2.$$

Proof: Using (3.15) and (3.16) we get that

$$\frac{Pe_1}{Pe_2} = \frac{\sum_{i=d}^{n} A_i\, p^i (1-p)^{n-i}}{\sum_{j=d+1}^{n-1} A_j\, p^j (1-p)^{n-j}}, \quad j \text{ even}, \ p \neq 0,$$

or

$$\frac{Pe_1}{Pe_2} = 1 + \frac{\sum_{v=d}^{n} A_v\, p^v (1-p)^{n-v}}{\sum_{j=d+1}^{n-1} A_j\, p^j (1-p)^{n-j}}, \quad v \text{ odd}, \ j \text{ even}. \qquad (3.17)$$

Since V_1' is invariant under a transitive permutation group, we have from Theorem 3.1 that

$\frac{A_{j-1}}{A_j} = \frac{j}{n+1-j}$. Substituting this result in the second term of (3.17) we obtain :

$$\frac{\sum_{v=d}^{n} A_v\, p^v (1-p)^{n-v}}{\sum_{j=d+1}^{n-1} A_j\, p^j (1-p)^{n-j}} = \frac{\sum_{j=d+1}^{n-1} \frac{j}{n+1-j} A_j p^{j-1} (1-p)^{n-j+1} + A_n p^n}{\sum_{j=d+1}^{n-1} A_j\, p^j (1-p)^{n-j}}$$

v odd, j even (3.18)

The expression (3.18) is greater or equal to 1 if each term of the numerator is greater than the corresponding term in the denominator. The fraction $\frac{j}{n+1-j}$ is minimum for $j = d+1$. Therefore (3.18) is greater than or equal to 1 if

$$\frac{d+1}{n+1-(d+1)} \quad \frac{(1-p)}{p} \geq 1 \qquad \text{or} \qquad p \leq \frac{d+1}{n+1}$$

Then $\frac{Pe_1}{Pe_2} > 2$

or $Pe_1 > 2\,Pe_2$ Q.E.D.

Theorem 3.4 holds for codes for which Theorem 3.1 holds. This includes [30] the Golay code, all quadratic residue codes and all primitive BCH codes and primitive cyclic Reed-Muller codes.

The condition stated in Theorem 3.4 for $Pe_1 > 2\,Pe_2$ is a sufficient condition but not a necessary one.

In Fig 3.27 we have plotted $\frac{Pe_1}{Pe_2}$ vs. p for the (15, 11) d = 3 and (15,7) d = 5 BCH codes. The figure shows that $\frac{Pe_1}{Pe_2} > 2$ for all $p \leq 1/2$, and that the improvement is greater as p becomes small.

From the above considerations we can conclude that a substantial gain in error detecting ability is possible through the use of even-weighted codes, particularly in channels with small p.

The price paid for this improvement is very small in that we loose one information bit, i.e. each codeword contains k - 1 bits of information. This is insignificant compared to the gain in error detecting capability.

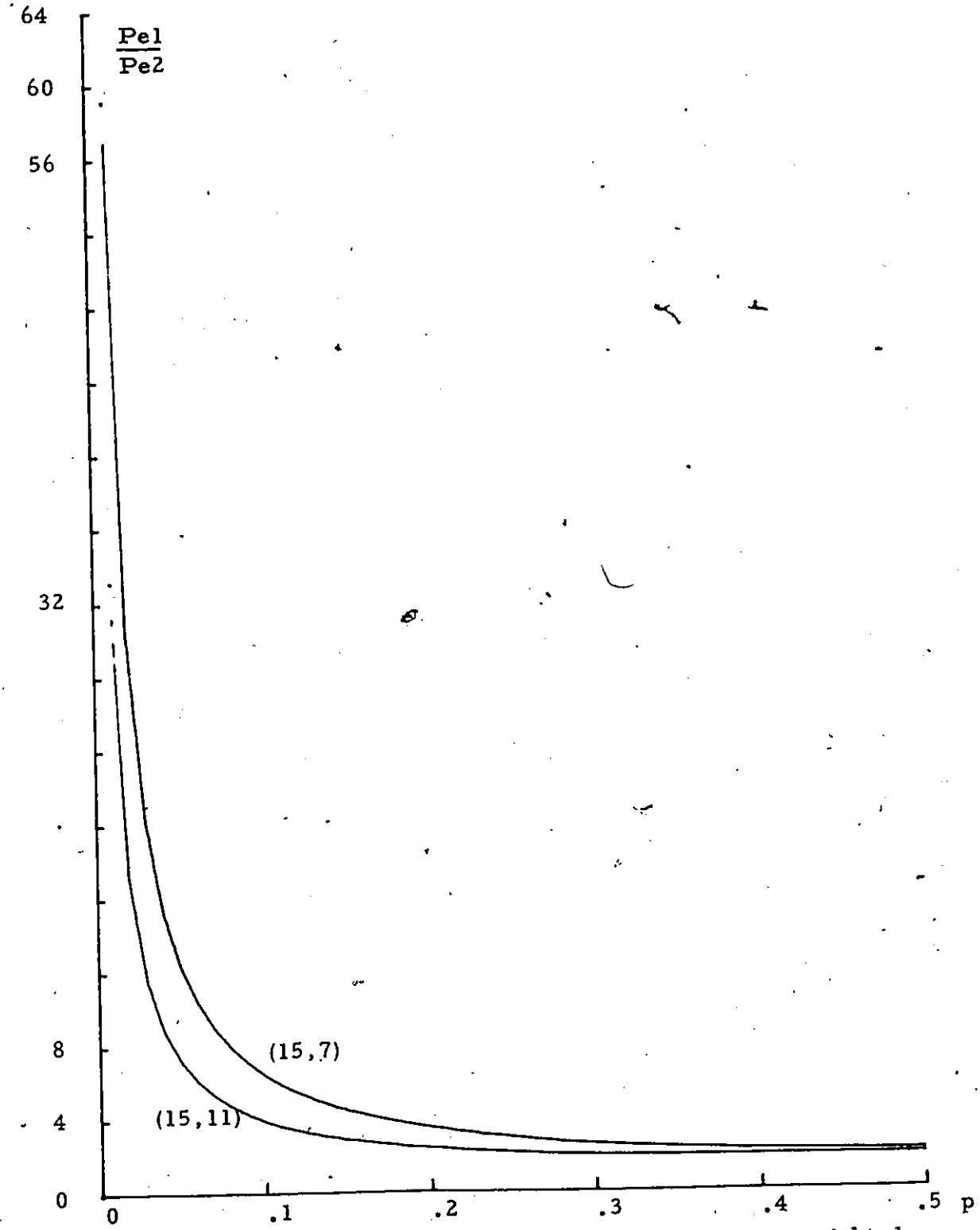

Figure 3.27 Improvement in Pe obtained by using the even-weighted subset of the (15,7)d=5 and (15,11)d=3 codes.

CHAPTER 4

CERTAIN CODES WITH ODD BEHAVIOR

4.1 INTRODUCTION

When dealing with the problem of undetected errors, we intuitively feel that Pe should be an increasing function of p. If the noise increases, we would naturally expect to have more undetected errors. But this is not always the case. For certain codes, Pe actually decreases as p is increased within a certain range of values of p. As examples of such codes we refer to Figures 4.1 to 4.6.

In these figures we have also plotted the approximation β. We observe that β fails to be a good approximation in the region where the code behavior is unusual. This is due to the fact that approximation β is an increasing function of p.

Fig. 4.7 is a plot of Pe and $\frac{dPe}{dp}$ vs. p for the (25,5) d = 5 BCH code. We observe that the derivative is negative in the region where Pe is decreasing.

Note that a horizontal line can intersect the plot of Pe in two places. What this means is that we can achieve the same error rate for two different values of p, that is, for two different signal to noise ratios. For example from Fig. 4.7 if a Pe of 3×10^{-6} is desired, the p required is either 0.08 or 0.385. If the present Pe is 10^{-5} which implies that p is approximately 0.125, then the desired Pe can be achieved by either increasing or decreasing the transmitted power. It would certainly be more economical to decrease the power transmitted.

In the next section we will discuss a class of codes that exhibit this property.

4.2 A CLASS OF CODES FOR WHICH P_e INCREASES WITH DECREASING p.

Consider the class of codes formed by interleaving $(n' = d, k' = 1)$ codes to degree d. The resultant code has the form $(n = d^2, k = d)$ and the generator polynomial is given by

$$g(x) = 1 + x^d + x^{2d} + \ldots + x^{(d-1)d}$$

An example of such a code is the (25, 5) $d = 5$ BCH code plotted in Figures 4.1 and 4.7. This code is formed by interleaving the (5, 1) code to degree 5.

We note that while as random-error correcting codes the rate is low for the d achieved, these codes can correct $\frac{n-k}{2}$ or less phased errors, or as single-burst-error detecting codes they can detect bursts of length $n-k$ or less. For example the (25, 5) $d = 5$ code can correct any two random errors, it can also correct 10 or less phased errors, or one random error and a burst error of length 5 or less, or a burst error of length 10 or less. It can also detect a burst error of length 20 or less. Hence these codes are optimum with reference to the Reiger Bound [29] which states that to correct a burst of length b, a code must have at least $2b$ check bits. Interpreting the condition $k = d$ in the light of the form of $g(x)$, we get

$$A_d = \binom{d}{1}, \quad A_{2d} = \binom{d}{2}, \quad \ldots, \quad A_{(d-1)d} = \binom{d}{d-1}, \quad A_n = 1$$

and all other A_i's, except A_o, are zero.

Using these numbers in (3.1) we obtain

$$Pe = p^n + \sum_{j=1}^{d-1} \binom{d}{j} p^{jd} (1-p)^{d(d-j)}$$

$$= [p^d + (1-p)^d]^d - (1-p)^{d^2} \qquad (4.1)$$

Differentiating (4.1) with respect to p, we get the derivative $\frac{dPe}{dp}$ to be

$$\frac{dPe}{dp} = d[p^d + (1-p)^d]^{d-1}[dp^{d-1} - d(1-p)^{d-1}] + d^2(1-p)^{d^2-1}$$

$$= d^2(1-p)^{d^2-1}[(m^d+1)^{d-1}(m^{d-1}-1) + 1]$$

$$= d^2(1-p)^{d^2-1}[1 - (1+m^d)^{d-1}(1-m^{d-1})]. \qquad (4.2)$$

We now prove the following

Theorem 4.1: The derivative $\frac{dPe}{dp}$ of (4.2) is negative at $p = \frac{1}{3}$ for $d \geq 4$.

Proof: With reference to (4.2) it is sufficient to show that

$$q(m) = (1+m^d)^{d-1}(1-m^{d-1}) > 1$$

at $m = \frac{p}{1-p} = \frac{1}{2}$ for $d \geq 4$.

We note that

$$q(m) = (1+m^d)^{d-1}(1-m^{d-1})$$

$$> q_1(m) = [1 + \binom{d-1}{1} m^d](1-m^{d-1})$$

$$= (1 + (d-1)m^d)(1-m^{d-1}).$$

Further,

$$q_1(\tfrac{1}{2}) = (1 + \frac{d-1}{2^d})(1 - \frac{1}{2^{d-1}})$$

$$= \frac{2^d + d - 1}{2^d} \cdot \frac{2^{d-1} - 1}{2^{d-1}}$$

$$= \frac{2^{2d-1} + d2^{d-1} - 2^{d-1} - 2^d - d + 1}{2^{2d-1}}$$

$$= 1 + \frac{d2^{d-1} - 2^{d-1} - 2^d - d + 1}{2^{2d-1}} \qquad (4.3)$$

With reference to (4.3), letting

$$q_2 = \frac{d2^{d-1} - 2^{d-1} - 2^d - d + 1}{2^{2d-1}}$$

and letting $d = 2 + \Delta$, we obtain

$$q_2 = \frac{\Delta 2^{d-1} - 2^{d-1} - (1 + \Delta)}{2^{2d-1}} . \qquad (4.4)$$

Now if $\Delta \geq 2$, or equivalently $d \geq 4$, we see that, in (4.4), $\Delta 2^{d-1} - 2^{d-1} \geq 2^{d-1} = 2^{1+\Delta}$ which is clearly greater than $1 + \Delta$. Thus, if $d \geq 4$ then q_2 is positive. Then, with reference to (4.3), $q_1(\frac{1}{2}) > 1$ and finally $q(\frac{1}{2}) > q_1(\frac{1}{2}) > 1$.

Q.E.D.

An implication of Theorem 4.1 is, of course, that P_e is drecreasing at $m = \frac{1}{2}$, or equivalently $p = \frac{1}{3}$, for the class of codes under consideration.

We also note that for $d = 3$,

$$q(m) = (1 + m^3)^2 (1 - m^2)$$

from which the derivative

$$q'(m) = 2m (1 + m^3) (3m - 4m^3 - 1).$$

It is easily verified that the roots of $q'(m)$ in the interval $0 < m \leq 1$ are $m = \frac{1}{2}$, $m = \frac{1}{2}$. Since $q(0) = 1$, $q(.5) = \frac{243}{256}$ and $q(1) = 0$, we can conclude that $q(m) \not> 1$ so that Pe of (4.1) is an increasing function of p. This means that for a code with $d = 3$ it is not possible for Pe to decrease as p increases.

Of the 6 codes presented in this chapter, only the (25,5) $d = 5$ BCH code belongs to the class of codes for which Theorem 4.1 applies. Probably there are more classes of codes for which Pe decreases with increasing p.

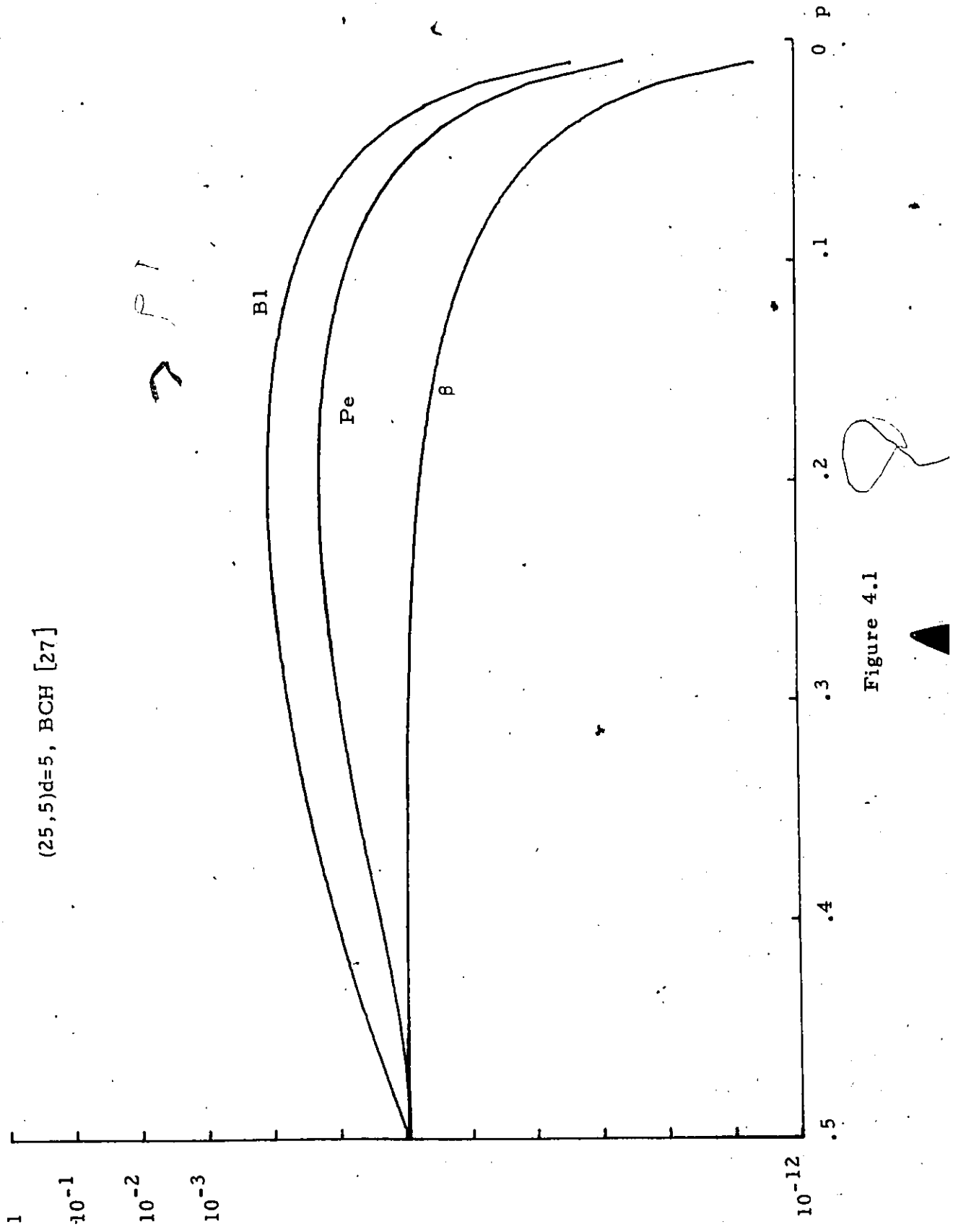

Figure 4.1

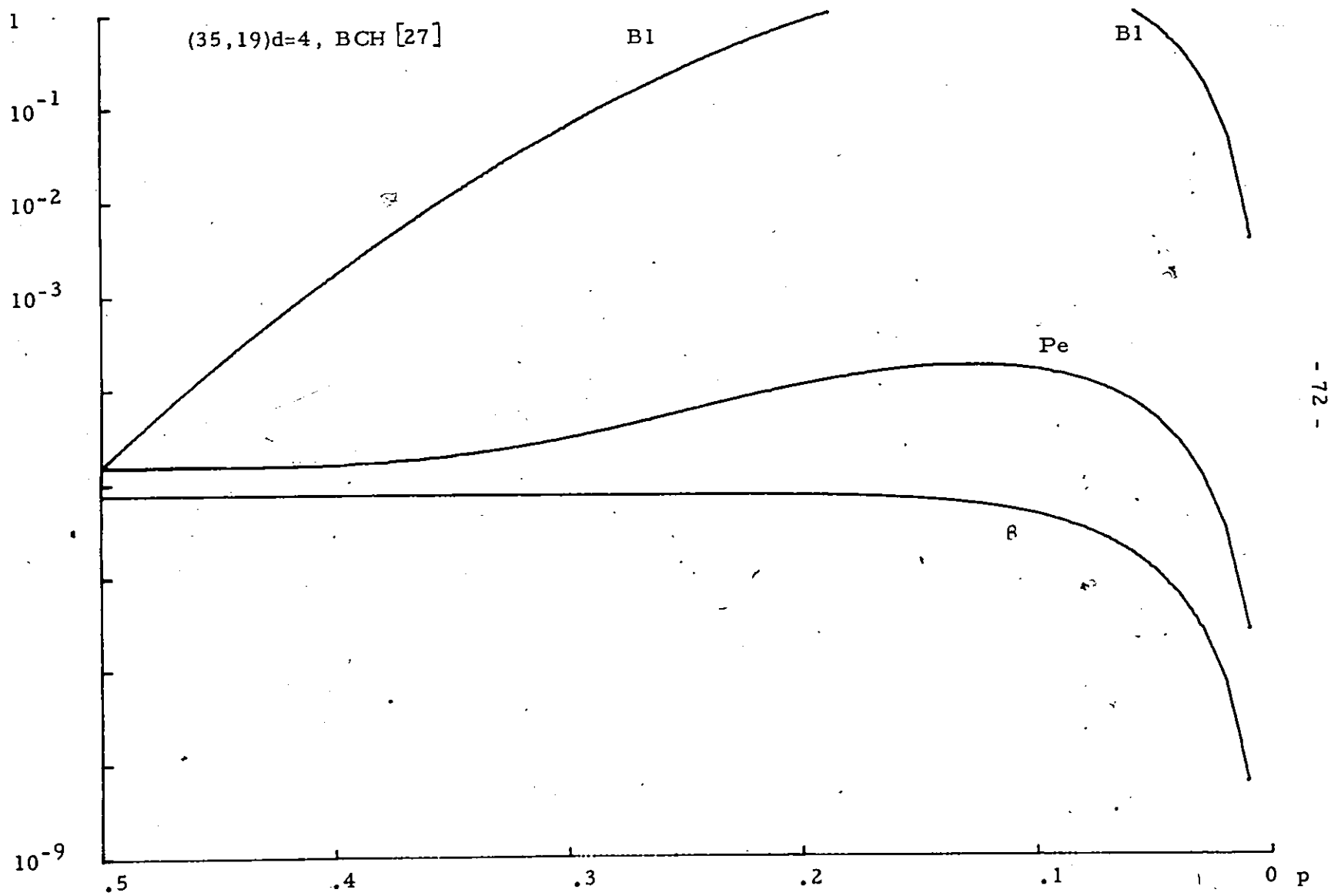

Figure 4.2

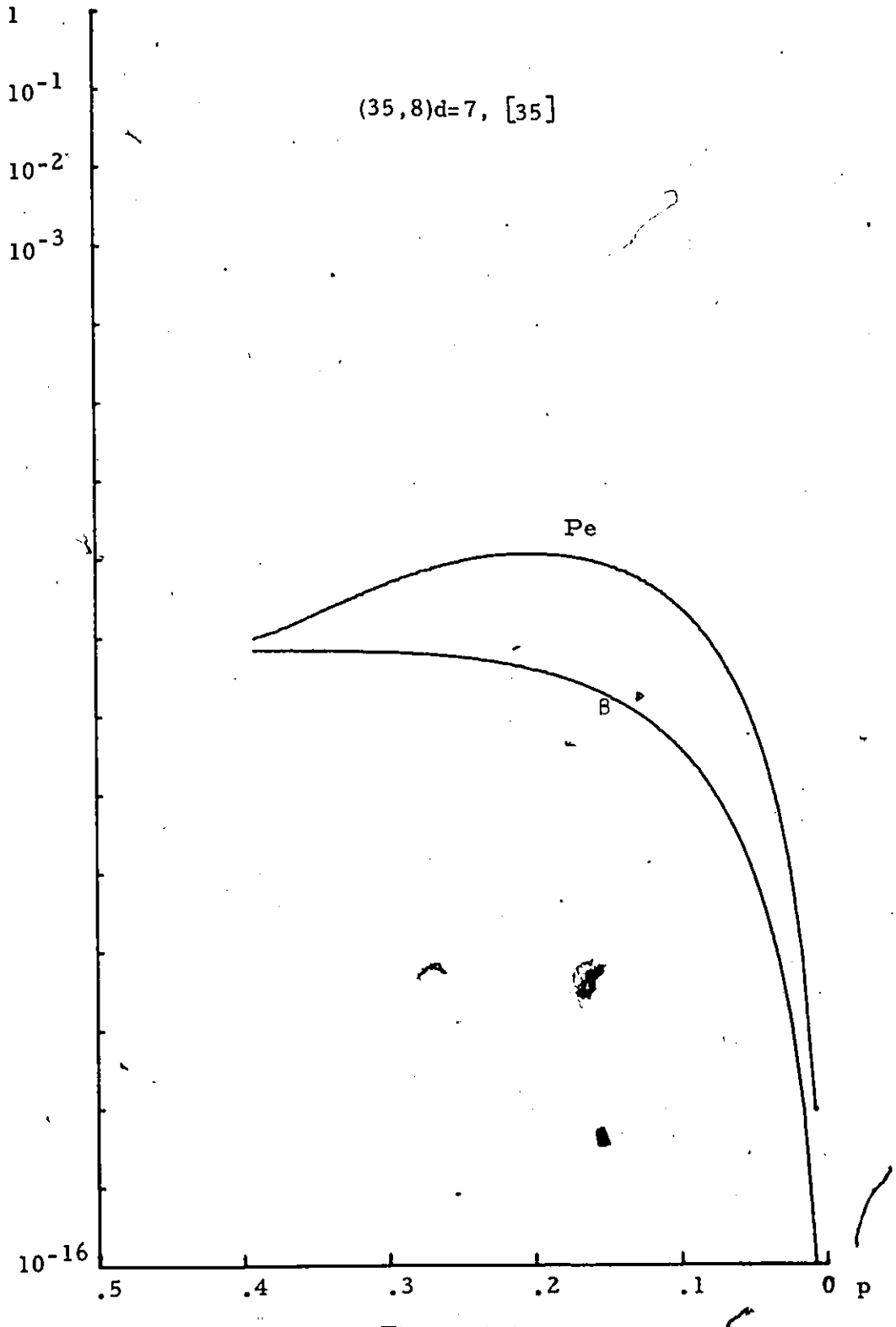

Figure 4.3

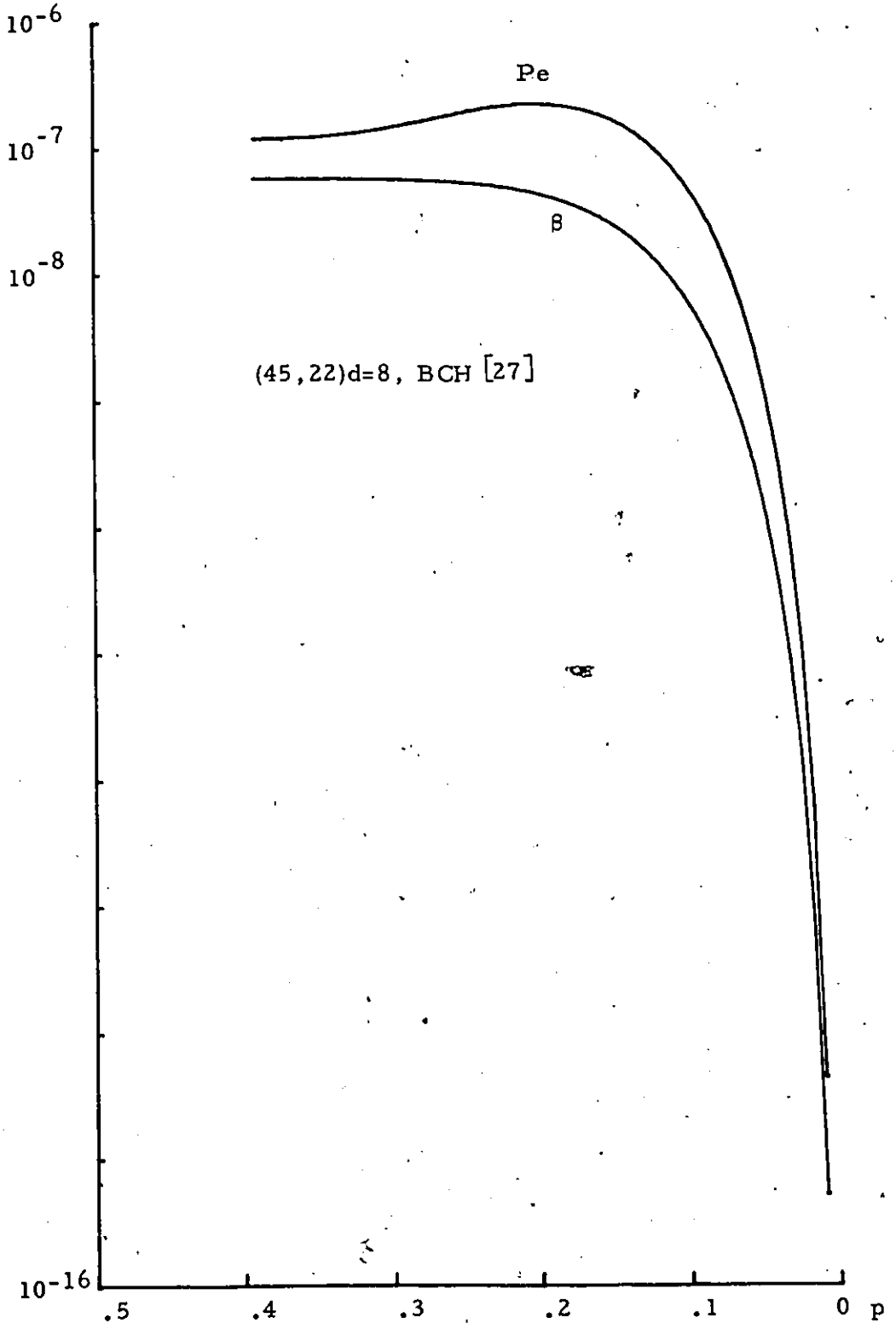

Figure 4.4

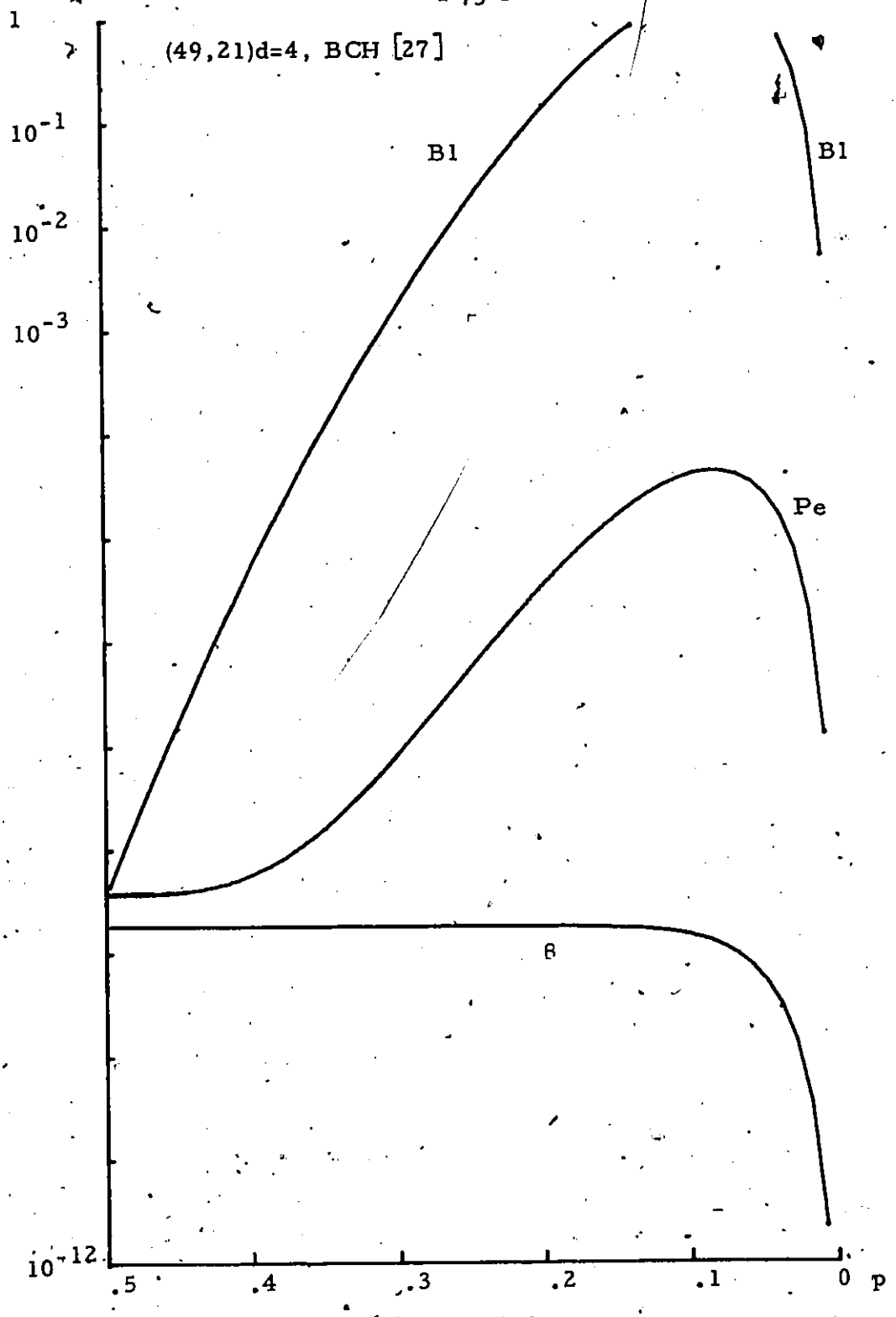

Figure 4,5

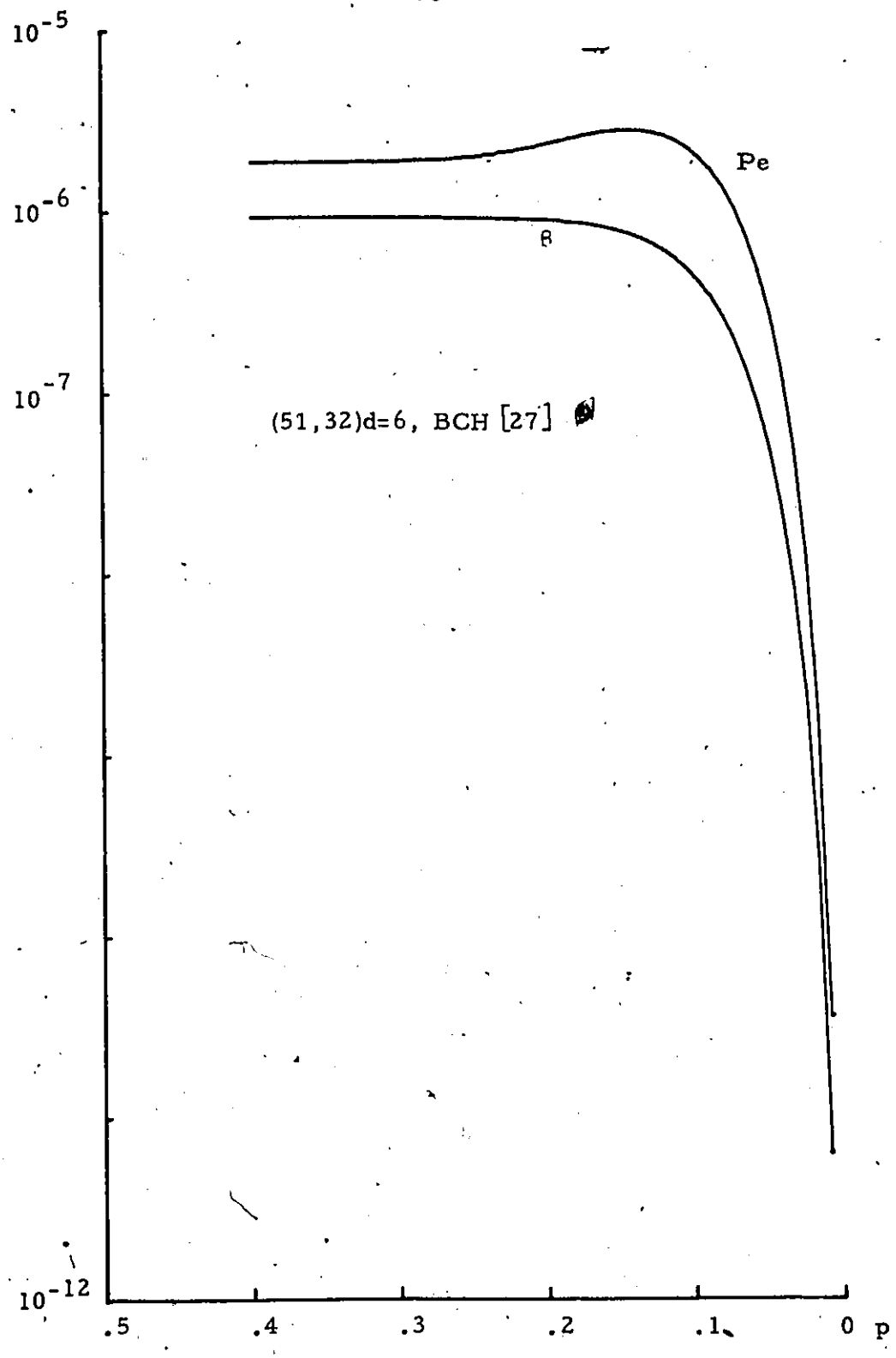

Figure 4.6

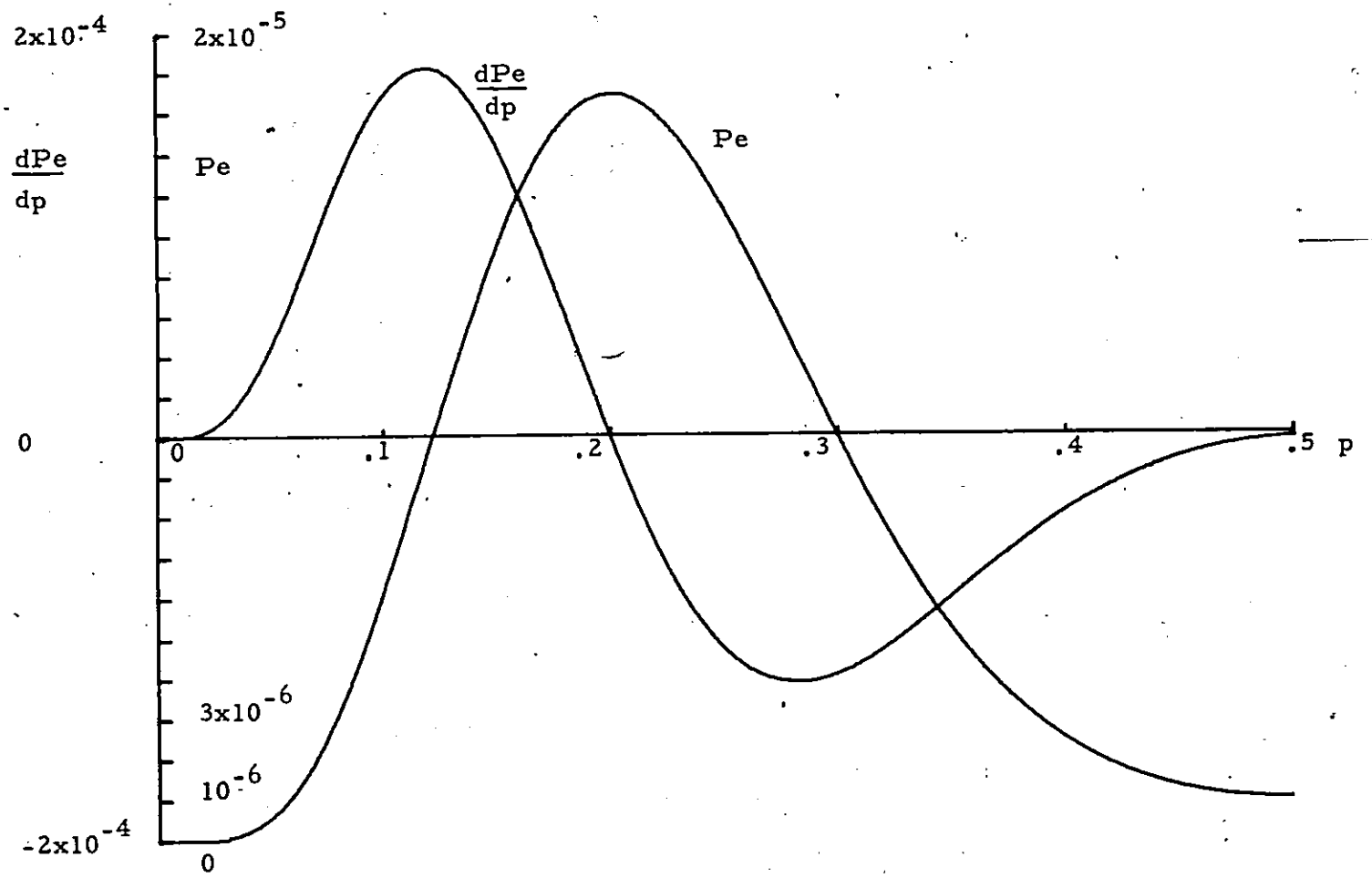

Figure 4.7 Pe and dPe/dp for the (25,5)d=5 BCH code.

CHAPTER 5

CONCLUDING REMARKS

In this thesis we have presented statistics of the error occurrence in the telecommunication network and given examples of how these statistics can be used when designing error control systems. We have briefly described the FEC and ARQ systems, considered their merits and concluded that ARQ systems are better suited for the telephone channel.

In chapter 3 we have considered the problem of estimating the probability of undetected errors when group error-correcting codes are used in the BSC for error detection without knowledge of the weight distribution of the code. The estimates presented are tight only for small values of p. Further work in this area should include an attempt to prove that the approximation β is a lower bound for Pe. More research should be done on weight distribution in codes. We have shown that knowledge of weight distributions is extremely important to any work done on error probabilities.

We also consider the fact that a substantial gain in error detecting ability is possible through the use of even-weighted codes, particularly in channels with small p. We show that the improvement given by the ratio $\frac{Pe_1}{Pe_2}$ (eq. (3.16)) is greater than 2 for $p \leq \frac{d+1}{n+1}$. It would be interesting to prove that $\frac{Pe_1}{Pe_2}$ will always be greater than 2 for $p \leq \frac{1}{2}$.

In chapter 4 we show that Pe can actually decrease in an appropriate interval of p depending on the code under consideration. Further investigation in regard to the weight distribution of codes for which this behavior of Pe occurs should prove worthwhile.

REFERENCES

[1] M. Eleccion, "A/D and D/A Convertors", IEEE Spectrum, Vol. 9, No. 7, July 1973, p. 63.

[2] R. J. Benice and A. H. Frey, Jr., "An Analysis of Retransmission Systems", IEEE Trans. Commun. Technol., Vol. COM-12, Dec. 1964, pp 135 - 145.

[3] R. J. Benice and A. H. Frey, Jr., "Comparisons of Error Control Techniques", IEEE Trans. Commun. Technol., Vol. COM-12, Dec. 1964, pp 146 - 154.

[4] W. W. Peterson and E. J. Weldon, Jr., "Error Correcting Codes", MIT Press, Cambridge, Mass., 1972.

[5] R. W. Lucky, J. Salz and E. J. Weldon, Jr., "Principles of Data Communications", McGraw-Hill, New York, 1968, Chap. 12.

[6] M. E. Hellman, "Error Detection Made Simple", in 1974 Int. Conf. Commun., Conf. Rec., pp 9A1 - 9A4.

[7] E. Y. Rocher and R. L. Pickholtz, "An Analysis of the Effectiveness of Hybrid Transmission Schemes", IBM J. Res. Develop., July 1970, pp 426 - 433.

[8] A. R. K. Sastry, "Performance of Hybrid Error Control Schemes on Satellite Channels", IEEE Trans. Commun. Technol., Vol. COM-23, No. 7, July 1975, pp 689 - 694.

[9] R. G. Gallager, "Information Theory and Reliable Communication", Wiley, New York, 1968, p 225.

[10] Peterson and Weldon, ibid, p. 299.

[11] Peterson and Weldon, ibid, p 64.

[12] A. A. Alexander, R. M. Gryb, and D. W. Nast, "Capabilities of the Telephone Network for Data Transmission", Bell Syst. Tech. J., Vol. 39, No. 3, May 1960, pp 431 - 476.

[13] R. L. Townsend and R. N. Watts, "Effectiveness of Error Control in Data Communications Over the Switched Telephone Network", Bell Syst. Tech. J., Vol. 43, No. 6, Nov. 1964, pp 2611 - 2638.

[14] C. W. Farrow and L. N. Holzman, "Nationwide Field Trial Performance of a Multilevel Vestigial Sideband Data Terminal for Switched Network Voice Channels", in Conf. Rec., 1968 IEEE Conf. Communications (Philadelphia, Pa.), June 12-14, pp 782 - 787.

[15] M. D. Balkovic, H. W. Klancer, S. W. Klare, and W. G. McGruther, "High-Speed Voiceband Data Transmission Performance on the Switched Telecommunications Network", Bell Syst. Tech. J., Vol. 50, No. 4, April 1971, pp 1349-1384.

[16] H. O. Burton and D. D. Sullivan, "Errors and Error Control", IEEE Proc. Vol. 60, No. 11, Nov. 1972, pp 1923 - 1301.

[17] A. B. Fontaine and R. G. Gallager, "Error Statistics and Coding for Binary Transmission Over Telephone Circuits", Proc. IRE, Vol. 49, June 1961, pp 1059 - 1065.

[18] J. L. Eisembies, "Conventions for Digital Communication Link Design", IBM Syst. J., Vol. 6, No. 4, 1966, pp 267-302.

[19] James Martin, "Teleprocessing Network Organization", Englewood Cliffs, N. J. Prentice Hall, 1970.

[20] D. Lignos, "Error Detection and Correction in Mass Storage Equipment", Computer Design, Oct. 1972, pp 71 - 75.

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

[22] S. Lin, "An Introduction to Error Correcting Codes," Prentice-Hall, Englewood Cliffs, N.J., 1970.

[23] H. O. Burton, "A Survey of Error Correcting Techniques for Data on Telephone Facilities", Bell Telephone Laboratories, Incorporated, Holmdel, N.Y. 07733.

[24] M. D. Balkovic and P. E. Muench, "Effect of Propagation Delay, Caused by Satellite Circuits, on Data Communications Systems That Use Block Retransmission for Error Correction", in ICC Conf. Rec., June 1969, pp 29 - 31 - 29 - 36.

[25] S. E. Tavares, B. K. Bhargava and S. G. S. Shiva, "Some Rate-P/(p+1) Quasi-Cyclic Codes", IEEE Trans. Inform. Theory, Vol. IT-20, Jan. 1974, pp 133 - 135.

[26] P. Robillard, "Some Results on the Weight Distribution of Linear Codes", IEEE Trans. Inform. Theory, Vol. IT-15, Nov. 1969, pp 706-709.

[27] H. D. Goldman, M. Kliman and H. Smola, "The Weight Structures of Some Bose-Chaudhuri Codes", IEEE Trans. Inform. Theory, Vol. IT-14, Jan. 1968, pp 167 - 169.

[28] Peterson and Weldon, ibid, Appendix D.

[29] S. H. Reiger, "Codes for the Correction of 'Clustered' Errors", IRE Trans., IT-6, 1960, pp 16-21.

[30] Peterson and Weldon, ibid, p 246 - 247.

[31] E. R. Berlekamp, ibid, p 428.

[32] Peterson and Weldon, ibid, p 121.

[33] J. M. Goethals, "Analysis of Weight Distribution in Binary Cyclic Codes", IEEE Trans. Theory, Vol. IT-12, 1966, pp 401-402.

[34] V. V. Rao and S. M. Reddy, "A (48, 31, 8) Linear Code", IEEE Trans. Inform. Theory, Vol. IT-19, Sept. 1973, pp 709-711.

[35] T. Kasami, "Some Lower Bounds in the Minimum Weight of Cyclic Codes of Composite Length", IEEE Trans. Inform. Theory, Vol. IT-14, Nov. 1968, pp 814 - 817.

[36] E.R. Berlekamp, ibid, p. 228.