mortality, this oldest age group has been extended to 100 years and over, with five-year age groups used between ages 80 and 100. To facilitate this extension, it is assumed that the force of mortality schedule (i.e., the curve of age-specific death rates) grows exponentially beyond age 80 to age 105.

Apart from these useful additions to the second edition, two others might have been possible. First, the actual or implied lower limit to the level of fertility might have been reduced to reflect the fertility decline in many industrial nations since the mid-1960's. In the "GRR set" of stable populations, the lowest value for the total fertility rate (equivalent to the average number of lifetime births per woman) is 1.64. In the "growth rate" set, the lowest value is approximately 1.54. However, by 1982 many developed countries had total fertility rates that had dropped to or below these levels. Among them are Belgium (1.60), Denmark (1.43), West Germany (1.40), Italy (1.57), Luxembourg (1.58), the Netherlands (1.49), Sweden (1.62), and Switzerland (1.55).

Second, some attention could perhaps have been given to immigration and emigration as sources of population change. As it is, the tabulations of stable populations assume populations closed to the influence of migration. Yet it is known that a constant number (and age composition) of immigrants to a population whose fertility is below replacement leads eventually to a stationary population (i.e., a population with a zero growth rate and a fixed age distribution). Tabulations of a limited range of such populations might have been useful. Moreover, even though decedents and emigrants are indistinguishable in terms of their impact on population growth and structure, it is unlikely that the age pattern of emigration is such that an empirical study of emigration's effect can be undertaken within one of the four existing families of model life tables. The subject of emigration is of more than academic interest; it is one of the chief ways that many small high-fertility Caribbean countries keep their populations in check.

Thomas J. Espenshade
The Urban Institute

Evolution in Age-structured Populations.

Brian Charlesworth. New York: Cambridge University Press, 1980. xiii + 300 pp. $44.50 ($13.50 paperback).

Many populations of plants and animals consist of individuals that are not constrained to reproduce only once or at a particular time of year. Such populations contain individuals of various ages and are thus said to be age structured. Although a substantial body of theoretical work on age-structured populations exists in mathematical demography, until the last decade and a half there was relatively little theory that incorporated genetic variability. This was a result partly of mathematical difficulties and partly of early studies by Norton, Haldane, and Fisher that led to some confidence that the easier theory, which had been developed for populations with separate or discrete generations, was extensible, with minor modifications, to age-structured populations. However, the early papers of Norton and Haldane only contained detailed analyses of particular cases, whereas Fisher's discussion in *The Genetical Theory of Natural Selection* purported to be more general but was vague and ambiguous.

One impetus to recent work, then, was to construct a sound and clear general theory so that implications of age structure were not neglected in interpreting data from real populations. Another was that such a mathematical structure was needed to assess and analyze new theories concerning the evolution of life histories, which had been proposed by Medawar and other biologists. Brian Charlesworth has been a leading figure in research in both the development of the general theory and its application to the study of the evolution of life histories. His is the first monograph to be published on demographic population genetics.

The book consists of four parts. The first is an introductory chapter on models of age-structured populations. It is mostly a discussion of the continuous- and discrete-time theories of population growth that were originally developed in detail by Lotka and Leslie, respectively.

The second part is Chapter 2, which generalizes two aspects of classical genetic theory for populations in which there is no selection. The first involves the approach to equilibrium of infinite populations that reproduce by random mating. The second generalization is a study of some effects of having a finite population with an unchanging size and demographic structure. Here two parameters are of central importance—the effective population number, N_e, and the generation interval, T. Research to date indicates that the usual stochastic theory for finite populations is then applicable, at least in the long run, if the appropriate N_e is used in place of the corresponding quantity for discrete generations and the unit of time is replaced by an appropriately chosen T.

The third part of the book consists of Chapters 3 and 4, which cover selection theory for age-structured populations. Some interesting effects of age structure are the dependence of genetic equilibria on demographic stability and the difference between appropriate measures of fitness of genotypes when populations are, or are not, at equilibrium.

The last part of the book is on the evolution of life histories. Two topics discussed are the evolution of senescence and conditions under which breeding once or breeding several times in a lifetime are favored.

The coverage is broad, including not only theory but many examples of applications of theory to data from real populations: The mathematical level is not very high. The material is, as the author states, accessible to anybody with a knowledge of basic calculus and matrix algebra. Although it is not stated, I think a knowledge of elementary population genetics, obtainable from a standard introductory text, is also needed. However, people interested in the subject matter of Charlesworth's book would presumably come to it with such knowledge. I think that the potential audience consists of experimental biologists, theoretical population geneticists, and students who have had one course in population genetics. The modest price of the volume should make it an attractive buy for the last group.

Because much of the theory has only been developed in the last decade and a half, gaps remain. For example, most of the theory discussed in Chapters 3 and 4 is based on the assumption that there is random mating with respect to age as well as genotype. The author admits that "effects of non-random mating with respect to age have not yet been satisfactorily dealt with." Another misgiving that I have is that all authors who have written on this subject, including myself, have made assumptions about fecundities that lead to linear recurrence equations for allele frequencies. This leads me to wonder whether there might not be biologically reasonable models under which the equations are nonlinear so that qualitatively different conclusions could emerge.

These remarks are not meant to be derogatory, for in my opinion a strength of this book is that the discussion is so clear, thorough, and honest that readers will be encouraged to make efforts to extend the theory, as well as to learn about its current status. I recommend this book to all who are seriously interested in the evolutionary theory of age-structured populations.

Edward Pollak
Iowa State University

Genealogical and Genetic Structure.

C. Cannings and E.A. Thompson. New York: Cambridge University Press, 1981. xi + 156 pp. $37.50 ($14.95 paperback).

This book is an introduction to the mathematics of genetic relationships. The first two chapters are devoted to methods of representing the genealogy of a group of individuals and the study of identity by descent and kinship and inbreeding coefficients, respectively.

Chapters 3 and 4 discuss gene identity and the evalution of allelic and genotypic variability in populations under regular and random mating systems. The classical approach to the study of such variability in populations is often via diffusion approximation of an underlying stochastic model of gene frequency. With a variety of examples, the authors make a convincing case that such problems are better attacked by explicit recognition of the central role of genealogy. The reader interested in some recent developments of this approach should see Kingman (1982), where the elegant structure of the genealogy of large haploid populations is uncovered.

Chapter 5 describes measures of genetic distance between individuals and populations and reviews methods for reconstructing genealogies on the basis of genetic data. Section 5.6 hints at intriguing statistical problems in the reconstruction of phylogenies on the basis of amino-acid sequence data and the estimation of divergence times. Felsenstein (1983) describes such problems in a manner accessible to statisticians.

The final chapter describes some of the algorithms necessary to compute coefficients of identity and likelihoods on pedigrees. Methods for simulating gene flow through a pedigree are also described. They provide one useful approach to the difficult problem of assessing the statistical behavior of genetic parameters estimated from such pedigrees.

This book is well written and carefully produced. The authors should be congratulated on providing mathematicians and statisticians with an excellent introduction to the difficult and challenging problems of genealogy.

SIMON TAVARÉ
Colorado State University

REFERENCES

FELSENSTEIN, J. (1983), "Statistical Inference of Phylogenies," *Journal of the Royal Statistical Society*, Ser. A, 146, 246–272.
KINGMAN, J.F.C. (1982), "On the Genealogy of Large Populations," *Journal of Applied Probability*, 19A, 27–43.

Cryptography: A Primer.

Alan G. Konheim. New York: John Wiley, 1981. xiv + 432 pp. $34.95.

I am certainly not an expert on the subject of cryptography. In fact, until the recent revolution in cryptography brought the subject into the open literature, I knew very little about the workings of real or proposed cryptographic systems. Even now, having followed much of the discussions on one-way functions, public key systems, NP-complete problems and other facets of the new cryptography, I still wonder if I really know anything about real cryptography.

I was therefore fascinated with the thought of reading *Cryptography: A Primer* by Alan Konheim. Though I knew that the current cryptographic systems used by the National Security Agency and the other classified agencies would remain inaccessible, I felt that the principles and practices of real cryptography would become apparent.

Konheim has tried hard to present the foundations of cryptography. He begins with simple substitution ciphers and progresses through the complexity of the famous Enigma system and sophisticated classical cryptographic techniques. Recent results from the new cryptography, such as public key systems, are also included. In Part 1, which deals with the presentation of classical concepts, the emphasis is on code breaking—an attack on a cryptographic system. The mathematical tools specific to each system are presented with detailed examples of their use. The probabilistic and information theoretic measures of cryptographic systems' resistance to attack are developed and discussed in the context of natural English language redundancy. Part 2, devoted to the new cryptography, presents techniques and their mathematical foundations that have been developed within the last seven or eight years. Since this is an active field, much of this section will need revision in later editions. Konheim also includes a chapter at the end of Part 2 on a specific IBM cryptographic system, Information Protection System (IPS). I feel that this is the weakest section in the book and adds little to the presentation.

It is difficult to determine the audience to which the book is directed. As a book that covers the basic elements of the subject of cryptography, it is indeed a primer. It is not, however, elementary in the sense of being accessible to anyone with a curious interest in cryptography. It is a mathematics book, and anyone used to the definition–theorem–proof style of mathematics will be comfortable with it. Those not at ease with this style will find the book difficult to read. Unfortunately I believe that many computer science students and engineers are uncomfortable with this form. When used as a textbook with the benefit of an instructor to introduce the various topics and to control the pace, the mathematical presentation should be satisfactory. On its own, however, the book has a definite lack of structure. For independent use by those who are neither cryptographers nor research mathematicians, the presentation would benefit greatly by a clearer separation of definitions, concepts, and results from the theorems, proofs, and symbology of the mathematical foundations.

The book is nearly self-contained. Although the subject matter uses results and techniques from many areas of mathematics, the necessary background material is always included. Specifically, the required definitions and results from probability, linear algebra, information theory, and number theory are presented as needed in the exposition. There is a separate appendix devoted to concepts of probability theory, and the results from the other areas are interwoven into the discussion. This makes for a slight unevenness in the presentation—for example, linear algebra (including an example of Gaussian elimination) is introduced and summarized in the course of discussing substitution ciphers. This is a trade-off an author has to make, and Konheim has chosen completeness at the risk of unevenness.

To some extent this book satisfied my expectations, but not completely. In part the fact that I am not entirely satisfied by this book is my responsibility. The author can certainly not be faulted for not writing the book I wanted to read. In other ways, however, I feel that the book could have been improved within its own scope and objectives. I would have preferred, perhaps, less detail and more insight. Although the mathematical foundations of cryptography are presented clearly, there is still a feeling that there are general principles and intuitive concepts that have been neglected.

Cryptography: A Primer is well edited. There are few typographical errors, and none of any serious consequence. This is typical of Wiley publications, but it must also represent a considerable devotion to detail by the author.

In summary, I feel that *Cryptography: A Primer* is a very ambitious book in which the author tried to include all of his favorite topics in cryptography. The result is a complete presentation that unfortunately lacks a clear direction and level. I believe that with diligent attention to the details of the examples, and perhaps several readings of the mathematics, a newcomer can learn much of the substance of cryptography. If the reader is not comfortable with the style of mathematical exposition, however, he will be left with little intuitive understanding.

WILLIAM J. ROSENBERG
Lockheed Palo Alto Research Laboratories

Contributions to the Sample Survey Theory.

V. Čermák, J. Henzler, and E. Ollé. Prague: State Pedagogical Publishing House, 1982. 104 pp. 15.50 Kčs.

This book consists of four papers in classical sampling theory. They are summarized briefly, since the book may not be widely available in North America.

1. "Another Way of Deriving the Expectations of Sample Central Moments" (Čermák)

Expectations of sample central moments of orders 2, 3, and 4 under simple random sampling with and without replacement are derived. The derivation is based on generalizations of the difference form of the sample second moment, namely

$$\left[\sum_{i\neq i'}^{n}\sum^{n}(y_i - y_{i'})^2\right] \Big/ 2n^2.$$

The result for order 2 is discussed in relation to difference forms (e.g., Yates, Grundy, and Sen) for the estimates of variance of the mean estimator under unequal probability sampling.

2. "The Use of the Difference Estimator in Repeated Sample Surveys" (Čermák)

It is shown that for sampling on successive occasions, the difference estimator (for the current time mean, using the previous time estimate and previous and current sample values) has almost as small a variance as the regression estimator under the optimal replacement policy.

3. "On Some Modifications of Systematic Sampling" (Henzler)

The main modifications considered are multistep systematic sampling (the sizes of successive intervals in the sample are $k_1, k_2, \ldots, k_r, k_1, k_2, \ldots, k_r, \ldots$), multiple systematic sampling (several random starts are employed), and two-part systematic sampling (circular systematic sampling is used with the sampling interval changing partway through). The performances of these designs are compared in the presence of linear trend, in the presence of periodicity, and for some natural populations.

4. "Theoretical and Empirical Comparisons of Some Unbiased and Almost Unbiased Ratio Estimators" (Čermák and Ollé)

The paper begins with a review of the literature up to 1974 on ratio estimators (including the estimators of Hartley-Ross, Mickey, Sastry, Cochran, Pascual, Murthy-Nanjamma, Quenouille, Beale, and Tin) and their estimates of MSE under simple random sampling. In the remainder of the paper, some empirical studies with sample size 3 from artificial