STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

DR 9

Mathematics and computing.

(Symposium on automatic digital computation, N.P.L., Teddington 1953, paper 17).

A. van Wijngaarden.

1953

Printed at the Mathematical Centre, 49, 2e Boerhaavestraat, Amsterdam.

The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O), by the Municipality of Amsterdam, by the University of Amsterdam, by the Free University at Amsterdam, and by industries.

N A T I O N A L P H Y S I C A L L A B O R A T O R Y

Paper No.17

SYMPOSIUM ON AUTOMATIC DIGITAL COMPUTATION

MATHEMATICS AND COMPUTING

by

A. van Wijngaarden.

- - - - - - - - - - -

A peculiar interaction takes place nowadays between mathematics in general and its remarkable offshoot that forms the topic of this conference, viz. highspeed computing. Of course, a good deal of interference already exists between mathematics and ordinary computing but high speed computing asks for new mathematical methods and also makes it possible to use already existing methods that were declared obsolete because they are impractical for ordinary calculations. High speed computing acts therefore on one side as a stimulus to mathematics whereas on the other side the computer may profit from the large reservoir of mathematical knowledge already in existence.

It is not my intention to discussfully all consequences of the impact of highspeed computing on mathematics or vice versa but I shall restrict myself to some special topics in this field mostly in connection with work that has been done at the Mathematical Centre at Amsterdam.

First of all I should like to emphasise that mathematics is more than analysis and algebra and that in principle other fields of mathematics might be of comparable use to computing. But, of course, the computer who does other work than sheer arithmetic and elementary algebra is more likely to come into contact with analysis than with anything else. And already in the application of analysis to computing many interesting points arise. Perhaps the most important tool that analysis provides the computer with is the calculus of finite differences. At first sight this looks less highbrow than the infinitesimal calculus, dealing with infinitely small differences but in reality it lies much deeper and forms actually a rather advanced topic in the theory of complex functions. The fact that it is so difficult is the reason that not very much is known in comparison to the situation in ordinary calculus. This provides an interesting source of uncertainty about our results.

One of the most prominent applications of the calculus of finite differences to computing is the theory of numerical interpolation, integration, and so on. An interpolated or integrated value of a function is represented as a linear combination of tabular entries, either directly in which case we speak of Lagrangean type formulas or in two steps in that first certain simple linear combinations of the entries are formed, so called differences of various orders, after which process the result is formed as a linear combination of one or two entries and a number of differences of increasing orders. The coefficients by which these differences have to be multiplied tend to zero rather rapidly in general. As long as only a finite number of terms are used both methods are equivalent apart perhaps from rounding off errors. The computer can only use, of course, a finite number of terms, and the question arises: "How many terms?" This is a very interesting question with a lot of aspects. First of all, it might perhaps not be superfluous to emphasise the fact that in general not an arbitrary accuracy can be obtained by taking more terms into account if at the same time the "step" i.e. the increment of the argument of the entries is kept constant. In general the series diverges, and if it happens to converge it is an extreme coincidence if the sum is the result that one wants to obtain. Therefore, one has to be modest in the number of terms. Under certain rather weak

/restrictions

restrictions the error committed by stopping after n terms in all these types of processes is equal to the product of three factors. The first factor is a rather irrelevant with increasing n decreasing function of the spot at which one interpolates and so on, the second is the n-th power of the step and the third is the derivative of order n+a (a being some constant) of the manipulated function somewhere in the interval determined by the arguments used in the process. From this observation one can prove the following general statements. The greater the step the more necessary, dangerous and inefficient is the use of higher differences. The smaller the step the more superfluous, harmless and efficient is the use of higher differences.

If smaller steps are used in integration, say, obviously a large number of them have to be taken in order to reach the aim. If high-speed computers are used, there are no direct objections against the use of very small intervals. This is a very nice situation. All remainderterms decrease enormously in size. Either one can increase the accuracy considerably in this way or one can abstain from the use of differences of high order. In the last case one gets instead of higher accuracy something else of high value, viz. ease of programming. The tendency towards ease of programming may here and in similar cases easily go so far that one only accepts the crudest methods that are only possible. In order to keep the accuracy constant one has then to decrease the step extremely. Not only does this decrease the efficiency of the high-speed computer but it also may introduce errors of another type, viz. those due to rounding off. Moreover in cases where all entries have to be stored as e.g. in the solution of elliptic partial differential equations, the required storage space may easily become prohibitive.

Both these remarks point our attention to another branch of mathematics, viz. to statistics. The study of the phenomena due to rounding off errors follows lines closely related to those followed in mathematical statistics. It is of vital importance for modern computing and here a direct stimulus to mathematics comes from computing. This study is moreover rather interesting from a mathematical point of view also. Here again apparently simple problems need already powerfull tools of analysis and more than that, one fruitfully introduces geometrical and numbertheoretical concepts. The first results of general character reveal unexpected and peculiar phenomena.

The second difficulty mentioned, viz. that of the storage of many functionvalues in the solution of partial differential equations is, at least in principle, overcome in a remarkable way by the introduction of the diffusion analogy analysed years ago by Courant, together with the application of the Monte Carlo method. Here the close cooperation with the statistician is evident and the theory of the random walk is rapidly extending due to the stimulus of computing.

Another interesting point arises in connection with the Monte Carlo method connecting computing with the theory of numbers, viz. the generation of random digits and random numbers. Of course, one can make those by means of special electronic devices, the electronic coins, but it is much more interesting and also more practical with respect of the reproducibility of the gambling process to generate them by computing. The question arises then how to generate very long sequences of numbers or digits, "very long" meaning with a very long period of repetition of the same pattern. Moreover the numbers or digits must pass succesfully statistical tests for randomness. Several schemes of construction have been devised, the first failing completely. A proper method has been indicated by Lehmer, who defines the sequence by the congruence $u_n = a\, u_{n-1} \pmod N$, $0 < u_n < N$. Each number is completely determined by its predecessor, and as there only N numbers different modulo N, the sequence is periodic and its period is less than N. If one chooses a arbitrarily with respect to N, the period may be only a small fraction of N but corresponding to a given N there exists a maximum period and a can be chosen in several ways so that one obtains that maximum period irrespective of the value u_o. This is a pure numbertheoretical problem. I suggested some time ago the use of recurrent sequences of second or higher order. Indeed, if one defines the sequence e.g. by $u_n = u_{n-k+1} - u_{n-k}$, a term is defined

/ by its

by its predecessors, and therefore the first observation learns that the period is less than N^k. Now a number of which we only know that is less than N^k has a good chance to be considerably larger than a number that is less than N. The formation is moreover extremely simple, the simplest example being the Fibonacci sequence $u_n = u_{n-1}+u_{n-2}$, so that there was a good reason to investigate the matter in considerable detail. Extensive studies have since been made by several researchworkers at the Mathematical Centre and I think it a good example of real contact between mathematics and computing. The computer here yields the stimulus and some provisory theorems most likely to be true as a first working basis. The pure mathematicians have not only provided the correct proofs but they have done much more; they added a new chapter to pure mathematics at the same time of practical value to the computer. Moreover, each new practical application of number theory is of interest as such, as there are still people who think that numbertheory is impractical.

At this moment it is perhaps worth while to ask whether high speed computing can be of any value to pure mathematics, because number theory is then one of the most likely candidates to profit. There lies certainly a field open here. For instance, the search for particular numbers can be extended to a somewhat higher level what can, as usually, help to suggest conjectures that may be proved or disproved but usually remain open. For instance, the search for new Mersenne prime numbers has been a welcome pray for the fast computers and the computations performed on the SWAC have yielded interesting results. It would be of real theoretical interest, for example, to go a step further than could be handled by the SWAC in its present state, and to investigate the number $-1+2^{8191}$, for if this proved to be prime then a large amount of theoretical work should be justified in order to prove or to disprove the conjecture: If $m_2 = 2^{m_1}-1$ is a prime number, then $m_3 = 2^{m_2}-1$ is also prime. The validity of this conjecture would for instance imply a constructive proof of the existence of a prime-generating function.

Another helping hand can of course be lent by tabulating functions. There are people that do not appreciate that tablemaking, and therefore I shall specify somewhat by taking a specific example. Quite recently I developed a rather general transformation that enables to compute functions from their heavily diverging asymptotic expansions. This method is in itself not directly meant for highspeed computers but it has the peculiarity that for application one needs extensive tables of very peculiar functions (that have not to do with the special function that one wishes to compute, of course). The computation of these tables is an enormous task, and here the highspeed computer can render welcome help.

Quite apart from any applications of the computers, only their construction yields problems in many fields of mathematics. It is well known that the design of circuitry is up to a high degree equivalent to problems in formal logic. Boolean algebra or Aiken algebra form nowadays tools of the computerengineer. In general also all questions with respect to binary representation of digits or numbers suggest problems. For instance, a problem connected with error detecting and correcting codes is the following: How many configurations of n binary digits can be constructed that differ from each other in at least d digits? The solution is not known. It may be regarded as a problem in combinatorial algebra but it is also a geometrical problem in n dimensions: How many solid hyperspheres of diameter $d^{\frac{1}{2}}$ can be attached with their centres to the corners of a hypercube of unitsize? In this form it is closely related to a wellknown subject in modern geometry, viz. that of the closest packing of spheres.

Closely connected is the theory of switching functions. Many results in Aiken's tables of switching functions are really clarified by regarding from a geometrical point of view. If one defines a polytope formed by corners of a n-dimensional hypercube of unitsize oriented along the coordinate axes to be at its inside if the corners have not a coordinate in common and at its outside if they have then a reflection on the table of switching functions reveals the fact that for $n \geq 4$ there are regular isotopes that fit into the inside as well as

/in

in the outside, whereas for $n < 4$ they do not exist.

A third problem arises from a question of Aiken. If the decimal system is to be used for a computer, and k parallel lines of binary digits are put available to represent decimal digits, then k is obviously at least equal to 4. Is it possible to derive a coding scheme, if necessary at the cost of a greater value of k, such that the sum digit and carry digit in the addition or multiplication of two decimal digits can be obtained, say, by simple permutations or more general by circuits of given simplicity. Duparc has analysed this and similar problems succesfully, but his proofs require concepts of grouptheory.

Van der Pol has dealt recently with problems related to the sum of the digits in any scale of the integral part of functions of x. The first results already are of a certain interest to computing and perhaps an interesting field is opened here. In general one might say that mathematics is quite well armed to answer succesfully the peculiar questions arising in highspeed computing. Of course, there are certainly fields in which a lot shall have to be done, e.g. in the theory of repetitive processes.

Mathematical Centre, Amsterdam,
University of Amsterdam.