Earliest Applications of the Computer at NSA*

BY SAMUEL S SNYDER

~~Secret~~

This paper describes the first successful application of an electronic computer in the solution of an Agency problem, namely the [National Bureau of] Standards Eastern Automatic Computer ("SEAC"). A flow chart of NSA's SEAC program is provided.

NSA's earliest successful application of electronic computers began in July 1950, before we had any computer. At that time, the only electronic computer in operation in this country was SEAC, recently completed at the National Bureau of Standards. In England, the EDSAC computer had been completed about a year before, and in this country the only computers being built commercially were UNIVAC, EDVAC, RAYDAC, and the Institute for Advanced Study machine (IAS computer). At NSA, our own ATLAS I (forerunner of the E R.A. 1101) was under construction at Engineering Research Associates' plant in St. Paul, and our ABNER was being built in our own Research and Development laboratories. Also, ABEL, the relay analog of ATLAS I, had been in use for about a year, mostly to check the logic of ATLAS I programs and for routine computations of statistical tables.

Responding to a request from Dr. A. Sinkov, then Technical Director in Communications Security, I met on July 11th, 1950, with him and [redacted] his deputy. They described an emergency requirement in COMSEC for production and checking of several hundred "involutory matrices." Each matrix consisted of 16 numbers, arranged in a 4×4 square and used in a Navy callsign system. The following requirements and limitations had to be satisfied in choosing and testing the entries:

1. Each entry to be chosen randomly, a nonzero positive integer between 1 and 36, inclusive.
2. All minors† of the generated 4×4 matrix to be unequal to zero modulo 37.

Perhaps a slight digression is in order for a few words about SEAC ("Standards Eastern Automatic Computer"). The decision by the

*Actually the predecessor agency -AFSA, Armed Forces Security Agency

†A minor is the evaluation, mod 37, of determinant of order less than that of the object matrix

Bureau of Standards to construct a computer in its own laboratories was made in August 1948. The Bureau had been acting in a technical liaison capacity, in connnection with the Bureau of Census' contract with Eckert-Mauchly Computer Corporation to construct the UNIVAC. A similar arrangement also existed for NBS to monitor the work by Raytheon Corporation on the first Raytheon computer (later known as RAYDAC) to be constructed for Navy's Bureau of Aeronautics. These functions probably represented the beginning of NBS interest in becoming a sort of government technical focal point in computer research. When the Bureau employed [redacted] (July 1948), this interest became focused, because of [redacted] intimate knowledge of EDVAC engineering and logic acquired during work on EDVAC at the Moore School of Electrical Engineering, University of Pennsylvania. At about the same time that NBS was considering constructing a computer, with supervision by [redacted] this agency's Army predecessor concluded an agreement with the Bureau providing, among other things, for the Bureau of Standards to contract for delivering mercury delay line memory for the computer, which we undertook to build. Our computer (ABNER) and the Bureau's machine (SEAC) were to be based on EDVAC logic and circuitry principles. SEAC's memory was only 512 words, however, whereas we early decided on the 1024-word size. Also, because of the Bureau pressure to finish their machine as soon as possible, the instruction repertoire was limited to only 8 instructions, compared with the 31 eventually built into ABNER. By July 1950, SEAC was getting into operation more or less regularly.

3. Produce the matrix and its inverse, which is the mod 37 inverse of the generated matrix.

During the week or two following the interview with Dr. Sinkov, Mr. L. W. Lathroum and I met with [redacted] and [redacted] of R&D, and received from them additional theoretical information bearing on matrix production and testing. Also, the possibility of using ABEL was considered, and rejected because it was too slow. I then spoke with [redacted] at the Bureau of Standards regarding the possibility of using the NBS machine SEAC. We also arranged for the generation of random numbers, required as input for the matrix production process by our Machine Production activity, using punched card techniques, with production of output punched paper tapes.

Although "Red" and I were both familiar with SEAC, we arranged a visit with Mrs. Ida Rhodes, senior programmer analyst at NBS, to obtain from her any specific operational details regarding programming and use of SEAC. The visit with Ida produced a single sheet (torn from an envelope!) containing all 8 SEAC instructions, handwritten in red pencil. She also told us about a few SEAC operating conventions, such as program preparation using hexadecimal notation (4-bit shorthand).

(b) (6)

Within a few weeks Red had written a preliminary program for producing involutory matrices on SEAC, using random numbers as input, and testing according to the criteria mentioned above. The program was converted from octal to hexadecimal notation, and checked. Also, during these first few weeks, formal arrangements were made for time on SEAC (usually Sundays or after midnight) and for transfer of funds from NSA to the Bureau of Standards to pay for SEAC time (at $24 per hour). Of course, we had the support of IBM equipment and specialists from our Machine Production Organization, in producing great masses of random numbers on punched paper tape. [redacted] and Dotty Blum were among those directly involved in this aspect of the job.

In the manual procedure for producing a matrix, we produced each entry by first calculating the number(s) which would make a 2×2 minor become zero and then arbitrarily assigning to that position any other number between 1 and 36. In carrying out the steps in such a process we followed the standard mathematical procedures applying to matrix manipulations and performed all multiplications and divisions modulo 37. Then, after a candidate "good" matrix was produced, we calculated its inverse.

When we used SEAC, the procedure differed from that for manual operations. Instead of calculating entries one by one, and testing each before accepting, we chose the set of 16 numbers from among those in our randomly-generated source and then applied the series of tests for nonzero minors. If a candidate matrix survived the tests, we printed it on the typewriter. The SEAC program took between 8 and 15 seconds per matrix, not counting output printing. This estimate includes time required to test and reject unsuccessful candidate matrices. Unfortunately, we do not have records showing actual estimates or proportion of rejections; the time estimate is based on personal diary entries reporting on amount of "good" operating time and number of matrices obtained. Figure 1 presents a flow chart of this operation.

Our experience in using SEAC seems, in retrospect, to have been a combination of frustration, exhilarating sense of accomplishment, and participation in making history. In July 1950 SEAC had been in operation only about one month, and many troubles still plagued the project. Furthermore, NBS engineers monopolized much of the machine time with tests and modifications to make it more reliable, with plans to add to its memory, and with improvements in input-output equipment. The rest of the "prime" time was monopolized by NBS programmers for training, in debugging programs, and in productive computation. The result was that we were permitted to use SEAC only at midnight shift or Sunday afternoons.

(b)(3)-P.L. 86-36

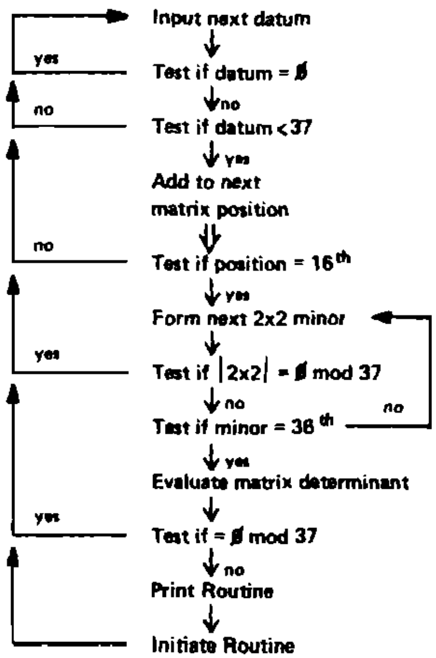

Fig. 1—Flow Chart of NSA's SEAC Program

Our first time on SEAC was Wednesday, August 23rd. In spite of the fact that SEAC's memory was misbehaving most of the time, we managed to get the program running far enough to check out some answers correctly. At the following session, we discovered a few errors in our program that were due to conversions from octal to hexadecimal notation, and corrected these. Also, SEAC memory troubles again plagued us; however, the next visit to SEAC, by Red Lathroum and John Rixse, produced some real results*. They put in about 16 continuous hours, of which an estimated 4½ hours of actual operation were

*On this occasion, Red Lathroum actually helped the Bureau account for some of the excessive "down" time when he noticed that some memory failures coincided with building air-conditioner switching times!

obtained, resulting in production of 374 matrices. After four or five more SEAC visits by [redacted] John Rixse, Dorothy Blum, Red Lathroum, and myself, a total of almost 900 matrices had been printed out and delivered to Dr. Sinkov.

During these sessions with SEAC, we had a number of Agency visitors who wanted to observe an electronic computer in operation. One of those most interested was [redacted] who was at this time in the process of rewriting some position descriptions in our section. Our discussions of the processes involved in computer programming engaged her interest, and her midnight trip to NBS to observe a live computer operation was the natural result. It should be added that we all learned more from "down" time on SEAC than from good operating time.

(b)(3)-P.L. 86-36