The checking of the accuracy of transmittal of telegraphic communications by means of operations in finite algebraic fields*

Lester Saunders Hill

March 5, 2015

Contents

*Unpublished notes, 40 pages, undated but probably written in mid- to late 1920s. These notes were typewritten, but mathematical symbols, tables, insertions, and some footnotes were often handwritten. These notes were LaTeX'd by David Joyner, who thanks Chris Christensen, the National Cryptologic Museum, and NSA's David Kahn Collection, for their help in obtaining these notes. Thanks also to Rene Stein of the NSA Cryptologic Museum library and David Kahn for permission to publish this transcription. Comments by transcriber will look his this: [This is a comment. - wdj]. The transcriber used Sage (www.sagemath.org) to generate the tables in LaTeX.

1 The problem considered

The forms of code in current use for the economical transmittal of cable and radio messages employ, almost uniformly, the so-called "pronounceable" combinations. "Pronounceability" is estimated in terms of letter groups which commonly occur in one or more of eight designated "telegraphic" languages: English, French, Spanish, etc. International regulations have, in fact, prescribed a system, of charges according to which a secret five-letter word is regarded, in the word count, as one-half of a telegraphic word, or as a full telegraphic word, according to as it is, or is not, pronounceable.

There is now discernible a definite tendancy to abandon this quite arbitrary pronounceability rule, which has heretofore hampered the development of code and cipher communication. And it seems not unlikely that, at some early session of the Interbational Telegraph Congress, all secret five-letter

combinations will be placed upon the same basis with respect to transmittal charges.

A mathematical problem of considerable scientific and practical interest arises in this connection. Messages written in pronounceable code or cipher contain within themselves certain checks upon the accuracy of their telegraphic transmittal. But sequences of unpronounceable groups will generally be quite arbitrary, and no such internal check will ordinarily be available. The outstanding requirement is some device capable of protecting totally unrestricted sequences, in a telegraphically economical way, against the hazards of faulty transmittal.

Let the finite set C of signs (letters, numerals, etc) upon which a given system of communication is based - plain-language, code, or cipher system - be placed in correspondence with the elements of a finite algebraic field F. Then the problem of checking sequences of signs in C becomes that of checking sequences of elements in F. As well-known, if we denote by Γ the number of elements, including the zero and unit elements, of a finite field F, then Γ is one of the numbers:

$$2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 29, 31, 32, \ldots,$$

that is to say, Γ is of the form $\Gamma = p^r$, where p denotes a prime positive integer greater than 1 and r denotes a positive integer. Conversely, if Γ is an integer of this form, we can very easily set up finite algebraic fields with Γ elements. In devising a scheme of checks for messages based upon the system C of communications with n distinct signs, we should normally work with a field F the number, Γ, of whose elements differs as little as possible form n. But this is not essential.

Our problem, viewed form the standpoint of mathematics, is simply that of providing economical and rigorous checks, easily applied in a practical way, upon the accuracy of transmittal of arbitrary sequences of elements in a finite algebraic field.

The method suggested will be applicable to telegraphic messages of any type: plain-language, code, cipher, cipher-code. It will, however, undoubtedly, be found susceptible of fundamental improvement in many respects; and it will probably yield to other, and more definitely practical, procedures that may subsequently be constructed be upon a basis of number-theoretical operations. The present paper will have served its purpose if it succeeds in directing attention to certain hitherto neglected practical possibilites inherent

in elementary algebraic manipulations.

2 Lemmas concerning algebraic fields

Familiarity with primary notions in the theory of finite algebraic fields, and of their algebraic extensions, will naturally be assumed here. Reference is made, however, to Steinitz [St], Dickson [D], Scorza [Sc]. But several points which will be needed very frequently in the following pages are summarized here in a series of lemmas. These lemmas assert properties of any algebraic field, whether it be finite or not.

Lemma 1 *Let F denote an algebraic field. Let the coeefficients a_{ij} in the system of equations*

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= 0 \\ &\vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n &= 0, \end{aligned}$$

be elements of F. Let Δ denote the value, in F, of the determinant

$$\begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \\ a_{n1} & \dots & a_{nn} \end{vmatrix}.$$

The system of equations has a solution other than

$$x_1 = x_2 = \cdots = x_n = 0$$

if and only if $\Delta = 0$.

Lemma 2 *Let F denote an algebraic field. Let the coeefficients in the system of equations*

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= 0 \\ &\vdots \\ a_{k1}x_1 + a_{k2}x_2 + \cdots + a_{kn}x_n &= 0, \end{aligned}$$

be elements of F, and let k be less than n. Then the system of equations certainly has a solution other than

$$x_1 = x_2 = \cdots = x_n = 0\,.$$

Lemma 3 *Let F denote an algebraic field. Let the a_{ij} and the c_i denote elements of F and let at least one of the c_i be different from zero. Consider the determinant*

$$\Delta = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \\ a_{n1} & \dots & a_{nn} \end{vmatrix}.$$

If $\Delta \neq 0$ then the system of equations[1]

$$\begin{gathered} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0 \\ \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n = 0, \end{gathered}$$

has one and only one solution.

Evidently, when solutions exist for the systems of equations considered in the forgoing three lemmas, such solutions lie entirely in the field F.

The lemma which follows is particularly useful. It is an immediate corollary of Lemma 1.

Lemma 4 *Let F denote an algebraic field. Let the a_{ij} denote elements of F. Then if*

$$\begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \\ a_{n1} & \dots & a_{nn} \end{vmatrix} = 0, \,.$$

we can determine at least one sequence of elements λ_1, λ_2, $\dots$, λ_n, which are not necessarily distinct but certainly are not all equal to zero, such that

[1]The case $\Delta = 0$ does not concern us.

$$\begin{gathered} a_{11}\lambda_1 + a_{21}\lambda_2 + \cdots + a_{n1}\lambda_n = 0 \\ a_{12}\lambda_1 + a_{22}\lambda_2 + \cdots + a_{n2}\lambda_n = 0 \\ \vdots \\ a_{1n}\lambda_1 + a_{2n}\lambda_2 + \cdots + a_{nn}\lambda_n = 0. \end{gathered}$$

Lemma 5 *The algebraic equation of nth degree*

$$a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0,$$

with coefficients in the algebraic field F, can not have more than n roots in F.

Most of the considerations of the present paper will depend, more or less directly, upon these five lemma.

3 Preliminary characterization of checking procedure

Our problem is to provide convenient and practical accuracy checks upon a sequence of n elements f_1, f_2, ..., f_n in a finite algebraic field F.

To fix the ideas, let us assume that we are to employ q-element checks c_1, c_2, ..., c_q upon the sequence f_1, f_2, ..., f_n. The checks are to be determined by means of a fixed reference matrix

$$Q = \begin{pmatrix} k_{11} & k_{12} & \dots & k_{1n} \\ k_{21} & k_{22} & \dots & k_{2n} \\ \vdots & & & \vdots \\ k_{q1} & k_{q2} & \dots & k_{qn} \end{pmatrix}$$

of elements of F, the matrix having been suitably constructed according to criteria which will be developed in the following pages. We send, in place of the simple sequence f_1, f_2, ..., f_n, the amplified sequence

$$f_1, f_2, \dots, f_n, c_1, c_2, \dots, c_q$$

consisting of the "operand" sequence and the "checking" sequence. The checking sequence contains q elements of F as follows:

$$c_j = \sum_{i=1}^{n} k_{ji} f_i,$$

for $j = 1, 2, \ldots, q$. Considerations of telegraphic economy dictate the assumption, made throughout the paper, that $q \leq n$.

Before laying down specifications for the reference matrix Q, we define a matrix of "index" q as one in which no q-rowed determinant vanishes.

4 Index of the reference matrix Q

There will be considerable advantage in employing a reference matrix Q of index q.

Consider the sequence $f_1, f_2, \ldots, f_n, c_1, c_2, \ldots, c_q$ which is to be transmitted. Errors may be made in transmittal, and the sequence may come through in the form

$$f'_1, f'_2, \ldots, f'_n, c'_1, c'_2, \ldots, c'_q\,,$$

where $f'_i = f_i + \epsilon_i$, $c'_j = c_j + \delta_j$, where $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, q$, the errors ϵ_i and δ_j being, of course, elements of the finite field F. If f_i (resp., c_j) is correctly transmitted then the error ϵ_i (resp., c_j) vanishes, and $f'_i = f_i$ (resp., $c'_j = c_j$).

Let us consider what happens when out sequence is mutilated to the extent of q errors, all of which affect the f_i (the c_j being supposed correctly transmitted).

There is no real loss of generality if we assume that the errors affect the first q of the f_i, the errors being $\epsilon_1, \epsilon_2, \ldots, \epsilon_q$. Since the c_j have been correctly transmitted, the mutilated message can not be in check unless

$$c_j = \sum_{i=1}^{q} k_{ji}(f_i + \epsilon_i) + \sum_{i=q+1}^{n} k_{ji} f_i = \sum_{i=1}^{n} k_{ji} f_i + \sum_{i=1}^{q} k_{ji}\epsilon_i.$$

But we recall that, by definition, $c_j = \sum_{i=1}^{n} k_{ji} f_i$. Hence the message will fail to check, and the presence of error will be disclosed, unless the q errors ϵ_i satisfy the system of equations

$$\sum_{i=1}^{q} k_{ji}\epsilon_i = 0 \tag{1}$$

for $j = 1, 2, \ldots, q$, of which the determinant is

$$\Delta = \begin{vmatrix} k_{11} & k_{12} & \ldots & k_{1q} \\ k_{21} & k_{22} & \ldots & k_{2q} \\ \vdots & & & \vdots \\ k_{q1} & k_{q2} & \ldots & k_{qq} \end{vmatrix}.$$

But our matrix is supposed to be of index q, so that $\Delta \neq 0$. It follows, by Lemma 1, that the system (1) has no solution other than $\epsilon_i = 0$, for $i = 1, 2, \ldots, q$. Hence q errors, confined to the f_i, can not escape disclosure if the reference matrix Q is of index q. By the same argument, applied a fortiori, a set of less than q errors, confined to the f_i, will certainly be disclosed when Q is of index q.

If the reference matrix Q is of index q, we can make the following statement:

Whenever the sequence $f_1, f_2, \ldots, f_n, c_1, c_2, \ldots, c_q$ is transmitted with errors not affecting the c_i, and not more than q in number, the presence of error will infallibly be disclosed.

We shall hereafter understand that Q is of index q.

5 The error distribution with at least q errors ϵ_i

Let the sequence[2]

$$f_1, f_2, \ldots, f_n,\ c_1, c_2, \ldots, c_q$$

be transmitted in the form

$$f'_1, f'_2, \ldots, f'_n,\ c'_1, c'_2, \ldots, c'_q\,,$$

containing $t \geq q$ errors which affect the f_i, and $h \geq 0$ errors which affect the c_j.

Let $t = q + s$. Then, to avoid discussing again the case already considered, we assume that at least one of the two integers s, h is greater than 0.

[2]Arbitrary error distributions will be considered later. Cf. sections 15, 16, 17, 18.

Let the errors among the c_j be δ_{j_1}, δ_{j_2}, ..., δ_{j_h}, affecting the c_{j_1}, c_{j_2}, ..., c_{j_h}. Without loss in generality, we may assume that the t errors affecting the f_i are ϵ_1, ϵ_2, ..., ϵ_t, so that the first t of the f_i are transmitted in error.

Suppose that the mutilated sequence is in full check. Then:

$$\sum_{i=1}^{t} k_{ji}(f_i + \epsilon_i) + \sum_{i=t+1}^{n} k_{ji} f_i = c_j + \delta_j$$

or

$$\sum_{i=1}^{n} k_{ji} f_i + \sum_{i=1}^{t} k_{ji}\epsilon_i = c_j + \delta_j$$

whence

$$\sum_{i=1}^{t} k_{ji}\epsilon_i = \delta_j$$

where $j = 1, 2, \ldots, q$ and where δ_j in c_j and may, of course, be equal to 0.

It follows that

$$\sum_{i=1}^{q} k_{ji}\epsilon_i = \delta_j - \sum_{i=1}^{t} k_{ji}\epsilon_i = b_j = \phi_j(\epsilon_{q+1}, \epsilon_{q+2}, \ldots, \epsilon_t, \delta_j),$$

where $j = 1, 2, \ldots, q$ and where ϕ_j denotes a polynomial in the errors $\epsilon_{q+1}, \epsilon_{q+2}, \ldots, \epsilon_t, \delta_j$.

The index of the reference matrix being q, the determinant

$$\begin{vmatrix} k_{11} & k_{12} & \ldots & k_{1n} \\ k_{21} & k_{22} & \ldots & k_{2n} \\ \vdots & & & \vdots \\ k_{q1} & k_{q2} & \ldots & k_{qn} \end{vmatrix}$$

of the systems of equations

$$\sum_{i=1}^{q} k_{ji}\epsilon_i = b_j \qquad (j = 1, 2, \ldots, q)$$

is not zero. Hence if all the b_j are equal to zero, Lemma 1 demands that all the ϵ_i, for $i = 1, 2, \ldots, q$, be equal to zero, contrary to hypothesis.

If at least one of the b_j is different from 0, Lemma 3 shows that $\epsilon_1, \epsilon_2, \ldots, \epsilon_q$ are uniquely determined as functions of the b_j, and therefore as functions of $\epsilon_{q+1}, \epsilon_{q+2}, \ldots, \epsilon_t, \delta_1, \delta_2, \ldots, \delta_q$:

$$\epsilon_i = \xi_i(\epsilon_{q+1}, \epsilon_{q+2}, \ldots, \epsilon_t, \delta_1, \delta_2, \ldots, \delta_q), \qquad (j = 1, 2, \ldots, q)$$

the functions ξ_i being, of course, rational functions. But, by assumption, all of the δ_j, except $\delta_{j_1}, \ldots, \delta_{j_h}$, vanish. Hence ϵ_i $((i = 1, 2, \ldots, q)$ is a rational function of $\epsilon_{q+1}, \epsilon_{q+2}, \ldots, \epsilon_t, \delta_{j_1}, \delta_{j_2}, \ldots, \delta_{j_h}$.

We conclude that if the mutilated message, containing $t + h$ errors, is to check up, so that the presence of error can escape detection, q of the errors must be carefully adjusted as rational functions of the remaining $t + h - q$ errors.

It is easy to measure the chance that mere accidents of erroneous telegraphic transmittal might effect this adjustment. Let Γ denote the total number of elements in the finite algebraic field F which we are dealing. When an error is made in transmitting a sequence of elements of F, the error may evidently have any one of $\Gamma - 1$ values – an error with the value 0 being no real error at all. It is therefore clear that our set of $t+h$ errors will enjoy only 1 chance in $(\Gamma - 1)^q$ of being accidentally adjusted so as to escape detection.

When $t = q + s$ errors occur among the f_i and h errors occur among the c_j in the transmittal of the sequence $f_1, f_2, \ldots, f_n,\ c_1, c_2, \ldots, c_q$, the errors being all of accidental telegraphic origin, the presence of error will infallibly be disclosed if $h = s = 0$; and will enjoy a 1-in-$(\Gamma - 1)^q$ of escaping disclosure if either of the two integers h, s is greater than 0.

This statement summarizes the results of the present section and those of section 4.

6 Arbitrary distrbution of errors affecting the f_i and the c_j

It is highly desirable, although not strictly necessary, to fashion the reference matrix Q in such a manner that every determinant contained in it, of every order, be different from zero.

Reference matrices of a practical type, and without a vanishing determinant of any order, may be construted in certain finite fields F by very direct

methods which can be more easily illustrated than described. It will be expedient at this poin, even at the expense of breaking the continuity of our discussion, to introduce concrete examples of operations in finite fields, and to show how reference matrices be conveniently set up in particular cases. The desirability of contriving that such matrices contain no vanishing determinant can then be brought out more effectively. The examination of arbitrary distributions of errors among the $n + q$ elements of a telegraphic sequence $f_1, f_2, \ldots, f_n, c_1, c_2, \ldots, c_q$ can be deferred, therefore, until later.

But, before going into details, we will describe the general form of reference matrix to be employed in all cases.

7 The general form of reference matrix

Let a_1, a_2, $\ldots a_n$ be n different elements of our finite field F, and let a_i be different from the zero element of F. Then we shall emply a reference matrix of the form

$$Q = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ a_1^2 & a_2^2 & \ldots & a_n^2 \\ \vdots & & & \vdots \\ a_1^q & a_2^q & \ldots & a_n^q \end{pmatrix}$$

or of the form

$$Q' = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ a_1 & a_2 & \ldots & a_n \\ a_1^2 & a_2^2 & \ldots & a_n^2 \\ \vdots & & & \vdots \\ a_1^{q-1} & a_2^{q-1} & \ldots & a_n^{q-1} \end{pmatrix}.$$

The actual procedure involved, and the real equivalence for checking purposes, of Q and Q', will presently be illustrated. We note here merely that each of the matrices Q, Q' is of index q. Let us examine Q'. A similar argument will be applicable to Q.

Suppose, for argument, that Q' contains a vanishing q-rowed determinant. Without loss of generality, we suppose that it is

$$Q' = \begin{vmatrix} 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_q \\ a_1^2 & a_2^2 & \dots & a_q^2 \\ \vdots & & & \vdots \\ a_1^{q-1} & a_2^{q-1} & \dots & a_q^{q-1} \end{vmatrix}.$$

Since this determinant is equal to zero, Lemma 4 guarantees the existence, in our field F, of the elements

$$\lambda_1, \lambda_2, \dots \lambda_q,$$

not all equal to zero, for which we may write

$$\lambda_1 + \lambda_2 a_i + \lambda_3 a_i^2 + \cdots + \lambda_q a_q^{q-1} = 0,$$

$(i = 1, 2, \dots, q)$. The a_i being, as assumed, all different, this implies that the equation

$$\lambda_1 + \lambda_2 x + \lambda_3 x^2 + \cdots + \lambda_q x^{q-1} = 0,$$

has q different roots in F, an implication which contradicts Lemma 5.

Thus Q' contains no vanishing q-rowed determinant, and if of index q. In the same way, Q may be shown to be of index q. But unless these matrices are constructed with care, they will, of course, generally contain vanishing determinants of various orders less than q. We defer for the moment the further consideration of this matter.

8 Examples of finite fields

The reader is probably accustomed to the congruence notation in dealing with finite fields. It may therefore be helpful to insert here two simple examples of finite fields, and to employ, in these concrete cases, the notations of the present paper rather than those of ordinary number theory.

Example 6 *A small field in which the number* Γ *is not prime.*

Let the elements of the field be the symbols or marks

$$0, 1, a, b, c, d, e, f, g;$$

and let us define, by means of two appended tables, the field of operations of addition and multiplcation in such a manner that the marks 0, 1 *represent respectively the zero and the unit elements of the field.*

These tables are

$+$	*0*	*1*	*a*	*b*	*c*	*d*	*e*	*f*	*g*
0	*0*	*1*	*a*	*b*	*c*	*d*	*e*	*f*	*g*
1	*1*	*a*	*0*	*c*	*d*	*b*	*f*	*g*	*e*
a	*a*	*0*	*1*	*d*	*b*	*c*	*g*	*e*	*f*
b	*b*	*c*	*d*	*e*	*f*	*g*	*1*	*a*	*0*
c	*c*	*d*	*b*	*f*	*g*	*e*	*a*	*0*	*1*
d	*d*	*b*	*c*	*g*	*e*	*f*	*0*	*1*	*a*
e	*e*	*f*	*g*	*1*	*a*	*0*	*c*	*d*	*b*
f	*f*	*g*	*e*	*a*	*0*	*1*	*d*	*b*	*c*
g	*g*	*e*	*f*	*0*	*1*	*a*	*b*	*c*	*d*

$\cdot$	*0*	*1*	*a*	*b*	*c*	*d*	*e*	*f*	*g*
0	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
1	*0*	*1*	*a*	*b*	*c*	*d*	*e*	*f*	*g*
a	*0*	*a*	*1*	*e*	*g*	*f*	*b*	*d*	*c*
b	*0*	*b*	*e*	*a*	*d*	*g*	*1*	*c*	*f*
c	*0*	*c*	*g*	*d*	*e*	*1*	*f*	*a*	*b*
d	*0*	*d*	*f*	*g*	*1*	*b*	*c*	*e*	*a*
e	*0*	*e*	*b*	*1*	*f*	*c*	*a*	*g*	*d*
f	*0*	*f*	*d*	*c*	*a*	*e*	*g*	*b*	*1*
g	*0*	*g*	*c*	*f*	*b*	*a*	*d*	*1*	*e*

Denoting by α *an arbitrary element of this field, we see that negatives and reciprocals of the elements of the field are as shown in the scheme:*

α	*0*	*1*	*a*	*b*	*c*	*d*	*e*	*f*	*g*
$-\alpha$	*0*	*a*	*1*	*e*	*g*	*f*	*b*	*d*	*c*
$1/\alpha$	-	*1*	*a*	*e*	*d*	*c*	*b*	*g*	*f*

The use of notations is easily illustrated. Thus, for example, we note that the determinant

$$\Delta = \begin{vmatrix} f & b & g \\ 1 & f & a \\ d & e & 1 \end{vmatrix}.$$

of the system of equations

$$\begin{aligned} fx + by + gz &= 0 \\ x + fy + az &= 0 \\ dx + ey + z &= 0 \end{aligned}$$

vanishes. For, expanding the determinant by the elements of its first row, we obtain

$$\begin{aligned} \Delta &= f(f - ea) - b(1 - da) + g(e - fd) \\ &= f(f + e) + e(1 + d) + g(e + b) \\ &= fc + eb + g(0) = fc + eb = a + 1 = 0. \end{aligned}$$

Hence the system has solutions other than $x = y = z = 0$. By the usual methods, it is quickly found that one solution is ($x = d$, $y = 1$, $z = 0$). The general solution is ($x = \lambda d$, $y = \lambda$, $z = 0$), where λ denotes an element of the field.

For further practice, we note that the system of equations

$$\begin{aligned} bx + gy &= d && (2) \\ ax + ez &= 0 && (3) \\ ex + fy + az &= f && (4) \\ & && (5) \end{aligned}$$

has exactly one solution. It may be found by the standard method employing quotients of determinants[3]*. or as follows:*
[11 lines of hand calculations are omitted. - wdj]
The solution is $x = y = f$, $z = c$.

As noted in Section 1, the number Γ of the elements of a finite algebraic field is either a prime integer greater than 1, or a positive integral power of such an integer. In the present example, we have $\Gamma = 9 = 3^2$. It may be observed in passing that if λ is any element of a finite field for which

$$\Gamma = 2^n, \qquad n \geq 1,$$

that is, for which Γ is a power of 2, then in that field $\lambda = -\lambda$.

[3]What we call today Cramer's rule - wdj.

Example 7 *A small field in which the number* Γ *of elements is prime.*

Let f_0, f_1, $\ldots f_{p-1}$ *be* p *symbols or marks, and let* p *be a prime integer. We readily define a finite algebraic field of which the elements are the* f_i. *To this end, we regard* f_i *as associated with the integer* i *which we shall call the "affix" of the mark* f_i. *Understanding that of course* 0 *is the "smallest integer" in any set of non-negative integers which includes* 0, *we now define as follows:*

Sum*: The sum of the marks* f_i *and* f_j *is given by the formula*

$$f_i + f_j = f_k,$$

where k *is the smallest non-negative integer satisfying*

$$i + j \equiv k \pmod{p}.$$

Product*: The product of the marks* f_i *and* f_j *is given by the formula*

$$f_i f_j = f_h,$$

where h *is the smallest non-negative integer satisfying*

$$ij \equiv h \pmod{p}.$$

With the operations of addition and multiplication thus defined, our set of p *marks constitutes, as is well-known, an algebraic field. We call a field of this type a "primary" field.*

In a primary field, an addition table would never be required. For we note that, if

$$f_{j_1}, f_{j_2}, \ldots, f_{j_t},$$

are t elements of our field then

$$\sum_{i=1}^{t} f_{j_i} = f_k,$$

where k is the smallest non-negative integer satisfying the congruence

$$\sum_{i=1}^{t} j_i \equiv k \pmod{p}\ .$$

Naturally, a similar statement holds for the product. We have

$$\prod_{i=1}^{t} f_{j_i} = f_h,$$

where h is the smallest non-negative integer satisfying the congruence

$$\prod_{i=1}^{t} j_i \equiv h \pmod{p} .$$

In the foregoing definitions, any of the terms of a sum, or of the factors of a product, may, of course, be equal.

When dealing with a primary field, we may obviously replace the marks of the fields by their affixes. We do this in the example which follows.

Example 8 *Let the marks of a finite field be*

$$0, 1, 2, \ldots, 21, 22,$$

the field containing $p = 23$ elements. An addition table is not needed. The multiplication table is as follows:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
2	2	4	6	8	10	12	14	16	18	20	22	1	3	5	7	9	11	13	15	17	19	21
3	3	6	9	12	15	18	21	1	4	7	10	13	16	19	22	2	5	8	11	14	17	20
4	4	8	12	16	20	1	5	9	13	17	21	2	6	10	14	18	22	3	7	11	15	19
5	5	10	15	20	2	7	12	17	22	4	9	14	19	1	6	11	16	21	3	8	13	18
6	6	12	18	1	7	13	19	2	8	14	20	3	9	15	21	4	10	16	22	5	11	17
7	7	14	21	5	12	19	3	10	17	1	8	15	22	6	13	20	4	11	18	2	9	16
8	8	16	1	9	17	2	10	18	3	11	19	4	12	20	5	13	21	6	14	22	7	15
9	9	18	4	13	22	8	17	3	12	21	7	16	2	11	20	6	15	1	10	19	5	14
10	10	20	7	17	4	14	1	11	21	8	18	5	15	2	12	22	9	19	6	16	3	13
11	11	22	10	21	9	20	8	19	7	18	6	17	5	16	4	15	3	14	2	13	1	12
12	12	1	13	2	14	3	15	4	16	5	17	6	18	7	19	8	20	9	21	10	22	11
13	13	3	16	6	19	9	22	12	2	15	5	18	8	21	11	1	14	4	17	7	20	10
14	14	5	19	10	1	15	6	20	11	2	16	7	21	12	3	17	8	22	13	4	18	9
15	15	7	22	14	6	21	13	5	20	12	4	19	11	3	18	10	2	17	9	1	16	8
16	16	9	2	18	11	4	20	13	6	22	15	8	1	17	10	3	19	12	5	21	14	7
17	17	11	5	22	16	10	4	21	15	9	3	20	14	8	2	19	13	7	1	18	12	6
18	18	13	8	3	21	16	11	6	1	19	14	9	4	22	17	12	7	2	20	15	10	5
19	19	15	11	7	3	22	18	14	10	6	2	21	17	13	9	5	1	20	16	12	8	4
20	20	17	14	11	8	5	2	22	19	16	13	10	7	4	1	21	18	15	12	9	6	3
21	21	19	17	15	13	11	9	7	5	3	1	22	20	18	16	14	12	10	8	6	4	2
22	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Products in which 0 is a factor all vanish, and therefore not shown in the table.

In any algebraic field, the elements λ and μ are negatives – $\lambda = -\mu$, $\mu = -\lambda$ – when $\lambda + \mu = 0$. In the present example, therefore, two marks i and j are negatives if

$$i + j \equiv 0 \pmod{23},$$

where i, j are momentarily regarded as ordinary integers of familiar arithmetic.

Negatives, reciprocals, squares and cubes are shown by the scheme:

λ	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
$-\lambda$	0	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
$1/\lambda$		1	12	8	6	14	4	10	3	18	7	21	2	16	5	20	13	19	9	17	15	11	22
λ^2	0	1	4	9	16	2	13	3	18	12	8	6	6	8	12	18	3	13	2	16	9	4	1
λ^3	0	1	8	4	18	10	9	21	6	16	11	20	3	12	7	17	2	14	13	5	19	15	22

This field will be called F_{23}. We shall use it in illustrating our checking operations.

Familiarity with the notations here employed may be gained by working out several exercises of simple type. Thus, the reader may note that the polynomial in F_{23}

$$x^3 + x^2 + 13x - 8,$$

has the three roots $x = 5, 6, 11$, so that we may write

$$x^3 + x^2 + 13x - 8 = (x + 18)(x + 17)(x + 12).$$

He may make the important observation that no two different elements of F_{23} have the same cube, and that this was to be expected. For the equation

$$x^3 - \lambda^3 = 0,$$

where λ denotes any element (other than 0) of F_{23} , can be written

$$(x - \lambda)(x^2 + \lambda x + \lambda^2) = 0,$$

the factor $x^2 + \lambda x + \lambda^2$ being irreducible in F_{23}. The fact that

$$x^2 + \lambda x + \lambda^2$$

has no root in F_{23} may be shown by "completing the square", and thus noting that the roots would have to be of the form

$$-\frac{\lambda}{2}(1 \pm \sqrt{-3}) = -\frac{\lambda}{2}(1 \pm \sqrt{20}).$$

But reference to the scheme of squares given above discloses that 20 is not the square of an element in F_{23}.

9 Introductory example of checking

We may use the field F_{23} as the basis for a simple illustrative exercise in the actual procedure of checking. The general of the operations involved will thus be made clear, so far as modus operandi is concerned, and we shall be enabled to discuss more easily the pertinent mathematical details.

It is easy to set up telegraphic codes of high capacity using combinations of four letters each which are not required to be pronounceable. In fact, a sufficiently high capacity may be obtained when only twenty-three letters of the alphabet are used at all. Hence we can omit any three letters whose Morse equivalents (dot-dash) are most frequently used. Let us suppose that we have before us a code of this kind which employs the letters

A B C E F G H I J L M N P Q R S T U V W X Y Z

and avoids, for reasons stated or for some good reason, the three letters

D K O .

Suppose that, by prearrangement with telegraphic correspondents, the letters used are paired in an arbitrary, but fixed, way with the thwenty-three elements of F_{23}. Let the pairings be, for instance:

A	B	C	E	F	G	H	I	J	L	M	N	P	Q	R	S	T	U	V	W	X	Y	Z
4	7	9	14	2	1	11	15	10	3	19	18	21	16	6	20	17	12	0	22	5	13	8

or, in numerical arrangement:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
V	G	F	L	A	X	R	B	Z	C	J	H	U	Y	E	I	Q	T	N	M	S	P	W

A four-letter group (code word), such as EZRA or XTYP, will indicate a definite entry of a specific page of a definite code volume, several such volumes being perhaps employed in the code. An entry will, in general, be a phrase of sentence, or a group of phrases or sentences, commonly occurring in the class of messages for which the code has been constructed.

Suppose that we have agreed to provide, in our messages, three-letter checks upon groups of twelve letters; in other words, to check in one operation a sequence of three four-letter code words. The twelve letters of the

three code words are thus expanded to fifteen; but we send just three telegraphic words – three combinations of five letters, each of which is, in general, unpronounceable.

For illustration, let the first three code words of a message be:

$$\text{XTYP} \quad \text{VZRV} \quad \text{HVHH}$$

The corresponding sequence of paired elements in F_{23} is:

$$5 \quad 17 \quad 13 \quad 21 \quad 0 \quad 8 \quad 6 \quad 0 \quad 11 \quad 0 \quad 11 \quad 11.$$

This is our operand sequence f_i (see §3):

$$f_1 = 5, \quad f_2 = 17, \quad f_3 = 13, \quad f_4 = 21, \quad f_5 = 0, \ \ldots, \ , f_{12} = 11.$$

Let us determine the checking matrix c_1, c_2, c_3 by using as reference matrix

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1^2 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 & 7^2 & 8^2 & 9^2 & 10^2 & 11^2 & 12^2 \\ 1^3 & 2^3 & 3^3 & 4^3 & 5^3 & 6^3 & 7^3 & 8^3 & 9^3 & 10^3 & 11^3 & 12^3 \end{pmatrix}$$

(see §7). Thus the c_j are to be

$$c_j = \sum_{i=1}^{12} i^j f_i \qquad (j = 1, 2, 3),$$

or

$$c_1 = \sum_{i=1}^{12} i f_i. \quad c_2 = \sum_{i=1}^{12} i^2 f_i. \quad c_3 = \sum_{i=1}^{12} i^3 f_i.$$

Referring to the multiplication table of F_{23} (§8, Example 6), we easily compute the c_j.

For the first element 5, of the operant sequence f_i, write

$$5 \quad 5 \quad 5$$

For the second element 17 place a sheet of paper (or a ruler) under the second row of the multiplication table, and in that row read: 11 in column 17, 22 in column 11, 21 in column 22. we now have a second line for the tabular scheme:

$$\begin{array}{ccc} 5 & 5 & 5 \\ 11 & 22 & 21 \end{array}$$

For the third element 13 place a sheet of paper (or a ruler) under the third row of the multiplication table, and in that row read: 16 in column 13, 2 in column 16, 6 in column 2. We now have the scheme:

$$\begin{array}{ccc} 5 & 5 & 5 \\ 11 & 22 & 21 \\ 16 & 2 & 6 \end{array}$$

The fifth, eighth, and tenth rows of the table will not be used, since $f_5 = f_8 = f_{10} = 0$. The complete scheme is readily found to be:

$$\begin{array}{cccc} 5 & 5 & 5 & \\ 11 & 22 & 21 & \\ 16 & 2 & 6 & \\ 15 & 14 & 10 & \\ 2 & 12 & 3 & \\ 19 & 18 & 11 & \\ 7 & 17 & 15 & \\ 6 & 20 & 13 & \\ 17 & 20 & 10 & \\ \hline 98 & 130 & 94 & \text{sum in } \mathbb{Z} \\ 6 & 15 & 2 & \text{sum in } F_{23} \end{array}$$

We have $c_1 = 6$, $c_2 = 15$, $c_2 = 2$.

We transmit, of course, the sequence of letters paired, in our system of communications, with the elements of the sequence,

$$f_1\ f_2\ \ldots f_{12}\ c_1\ c_2\ c_3.$$

Thus we transmit the sequence of letters: XTYP VZRV HVHH RIF; but we may conveniently agree to transmit it in the arrangement:

XTYPR VZRVI HVHHF ,

or in some other arrangement which employs only three telegraphic words (unpronounceable five-letter groups).

We could have used other reference matrices, but we shall not stop to discuss this point. We may remark, however, that if the matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1^2 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 & 7^2 & 8^2 & 9^2 & 10^2 & 11^2 & 12^2 \end{pmatrix}$$

had been adopted, the checking elements would have been

$$c_1 = \sum_{i=1}^{12} f_i. \quad c_2 = \sum_{i=1}^{12} i f_i. \quad c_3 = \sum_{i=1}^{12} i^2 f_i;$$

and their evaluation would have been accomplished with equal ease by means of the multiplication table of F_{23}.

10 Strength of the check applied in the example of section 9

We may inquire into the possibility of undisclosed errors occurring in the transmittal of the sequence:

f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	c_1	c_2	c_3
5	17	13	21	0	8	6	0	11	0	11	11	6	15	2
X	T	Y	P	V	Z	R	V	H	V	H	H	R	I	F

Invoking the theorem established in sections 4 and 5, and formulated at the close of §5, we may assert:

(1) If not more than three errors are made in transmitting the fifteen letters of the sequence, and if the errors made affect the f_i only, the c_j being correctly transmitted, then the presence of error is certain to be disclosed.

(2) If not more than three errors are made, all told, but at least three of them affect the f_i, then the presence of error will enjoy only a

$$1 - \text{in} - 22^3 \qquad (1 - \text{in} - 10648)$$

chance of escaping disclosure.

These assertions result at once from the theorem referred to. But a closer study of the reference matrix employed in this example permits us to replace them by the following more satisfactory statements:

(1') If errors occur in not more than three of the fifteen elements of the sequence $f_1 f_2 \dots f_{12} c_1 c_2 c_3$, and if at least one of the particular elements $f_{11} f_{12} c_2$ is correctly transmitted, the presence of error will certainly be disclosed. *But if exactly three errors are made, affecting presicely the elements* $f_{11} f_{12} c_2$, the presence of error will enjoy a 1-in-22^2 (1-in-484) chance of escaping disclosure.

(2') If more than three errors are made, then whatever the distribution of errors among the fifteen elements of the sequence, the presence of error will enjoy only a 1-in-22^3 (1-in-10648) chance of escaping disclosure.

Assertions of this kind will be carefully established below, when a more important finite field is under consideration. The argument then made will be applicable in the case of any finite field. But it is worthwhile here to look more carefully into the exceptional distribution of errors which is italicized in (1'). This will help us note any weakness that ought to be avoided in the construction of reference matrices.

Suppose that exactly three errors are made, affecting precisely $f_{11} f_{12} c_2$. If the mutilated message is to check up, and the errors to escape disclosure, we must have[4]:

$$11\epsilon_{11} + 12\epsilon_{12} = 0, \quad 11^2\epsilon_{11} + 12^2\epsilon_{12} = \delta_2, \quad 11^3\epsilon_{11} + 12^3\epsilon_{12} = 0.$$

These equations may be written:

$$11\epsilon_{11} + 12\epsilon_{12} = 0, \quad 6\epsilon_{11} + 6\epsilon_{12} = \delta_2, \quad 20\epsilon_{11} + 3\epsilon_{12} = 0.$$

But $11\epsilon_{11} = -12\epsilon_{12}$ can be written $11\epsilon_{11} = 11\epsilon_{12}$, or $\epsilon_{11} = \epsilon_{12}$. Etc. In this way, we find that the errors can escape disclosure if and only if

$$\epsilon_{11} = \epsilon_{12}, \quad \text{and} \quad \delta_2 = 12\epsilon_{11}.$$

The error ϵ_{11} can be made quite arbitrarily. But then the values of ϵ_{12} and δ_2 are then completely determined. There is evidently a 1-in-484 chance - and no more - that the errors will fall out just right.

[4]For error notations, see §4, 5.

The trouble arises from the vanishing, in our reference matrix, of the two-rowed determinant

$$\left| \begin{array}{cc} 11 & 12 \\ 11^3 & 12^3 \end{array} \right|.$$

Note that

$$\left| \begin{array}{cc} 11 & 12 \\ 11^3 & 12^3 \end{array} \right| = 11 \cdot 12 \cdot \left| \begin{array}{cc} 1 & 1 \\ 11^2 & 12^2 \end{array} \right| = 17 \left| \begin{array}{cc} 1 & 1 \\ 11^2 & 12^2 \end{array} \right| = 0,$$

since $11^2 = 12^2$.

From the fact that $\left| \begin{array}{cc} 11 & 12 \\ 11^3 & 12^3 \end{array} \right|$ is the only vanishing determinant of any order in the matrix employed, all other assertions made in (1') and (2') are readily justified. This will be made clear in the following sections.

It will be advantageous, as shown more completely in subsequent sections, to employ reference matrices which contain the smallest possible number of vanishing determinants of any orders.

11 Construction of finite fields for use in checking

Let F_Γ denote a finite algebraic field with Γ elements. It is well-known that, for a given Γ, all fields F_Γ are "simply isomorphic", and therewith, for our purposes, identical. We shall consequently refer, without restraint, tp "the field F_Γ."

If p is a prime positive integrer greater than 1, F_p is called, according to the terminology of Section 8, Example 8, a "primary" field. Explicit addition tables, as was noted in section 8, are hardly required in deal ing with primary fields. The most useful of these fields, in telegraphic checking, are probably F_{23}, F_{29}, F_{31}, and F_{101}. The field F_{101} will be considered in detail in what follows.

The number of elements in a non-primary finite algebraic field is a power of a prime. If we have

$$q = p^k$$

where p and k are positive integers greater than 1, and p is prime, the non-primary field F_q may be constructed very easily by algebraic extension of the field F_p. Explicit addition table is needed when working with a non-primary field. Otherwise, checking operations are exactly the same as in primary fields.

Example 9 The field F_3 with the elements (marks) $0, 1, 2$, has the tables

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

By adjoining a root of the equation $x^2 = 2$, an equation which is irreducible in F_3, we easily obtain the field F_9 with marks

$$\alpha j + \beta$$

where α and β denote elements of F_3. The marks of F_9 are thus

$$0, 1, 2, j, j+1, j+2, 2j, 2j+1, 2j+2.$$

These marks (elements) are combined, in the rational field operations of F_9, according to the reduction formula $j^2 = 2$. If we label the marks of F_9 as follows

0	1	2	j	$j+1$	$j+2$	$2j$	$2j+1$	$2j+2$
0	1	a	b	c	d	e	f	g

the addition and multiplication tables of the field are given as in Section 8, Example 7.

In a like manner, F_{27} can be obtained from F_3 by adjunction of a root of the equation $x^3 = x + 1$, which is irreducible in F_3 and F_9. The marks (elements) of F_{27} are

$$\alpha j^2 + \beta j + \gamma,$$

where α, β, γ are elements of F_3. They are combined, in the rational operations of F_{27} according to the reduction formula $j^3 = j + 1$.

Example 10 The field F_2 with the elements (marks) $0, 1$, has the tables

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

By adjunction of a root of the equation $x^5 = x^2 + 1$, which is irreducible in the fields F_2, F_4, F_8 and F_{16}, we easily obtain the field F_{32}. The marks of F_{32} are

$$\alpha j^4 + \beta j^3 + \gamma j^2 + \delta j + \epsilon,$$

where $\alpha, \beta, \gamma, \delta, \epsilon$ are elements of F_2; and these 32 marks are combined, in the rational operations of F_{32}, according to the reduction formula $j^5 = j^2 + 1$.

Example 11 The field F_5 with the elements (marks) $0, 1, 2, 3, 4$, has the tables

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

By adjoining a root of the equation $x^2 = 2$, which is irreducible in F_5, we readily obtain the field F_{25}. The marks of F_{25} are

$$\alpha j + \beta,$$

where α, β are elements of F_5; and these 25 marks are combined, in the rational operations of F_{25}, according to the reduction formula $j^2 = 2$.

Of the non-primary fields, F_{25}, F_{27}, F_{32} are probably those which are most amenable to practical application in telegraphic checking.

12 The field F_{101}

All essential points connected with the checking of telegraphic sequences by the methods proposed in this paper may be fully illustrated in one finite field. For our purposes, perhaps the most useful field is F_{101}, to which we shall confine our attention in the following sections.

The elements of the field F_{101} are the one hundred and one marks[5] 0, 1, 2, ..., 100. The operations of addition and multiplication are effected as explained in Example 8; and are abbreviated as suggested. To determine sums and products, we regard the marks of the field momentarily as integers of elementary arithmetic. Thus we have

$$\sum_1^n f_i = f_h, \qquad (\prod_1^n f_i = f_k),$$

the f_i being n marks of F_{101}, distinct or not, if, when the f_i are momentarily regarded as integers of elementary arithmetic, the congruence

$$\sum_1^n f_i \equiv f_h \pmod{101}, \qquad (\prod_1^n f_i \equiv f_k \pmod{101}),$$

holds.

It will not be possible to provide a full multiplication table for the field F_{101}. But the following special table will be found convenient.

Using the scheme of reciprocals shown in Table 1, we may easily perform an rational operations in F_{101}.

Example 12 Suppose, for example, that we wish to solve the system of equations[6]:

$$36x - 79y = 52, \quad 90x + 85y = 98.$$

They may be written

$$x - 79y/36 = 13/9, \quad x + 17y/18 = 49/45$$

[5]Hill actually uses the symbol X in place of 100.

[6]It happens that we shall not, in the remainder of this paper, have occasion to use the mark "X" of F_{101}. Hence, whenever an X occurs, it will be understood as variable, or "unknown", of ordinary equation theory. *Some symbol other than x ought perhaps to have been used for an element of* F_{101}. [Italicized statement was handwritten on the manuscript near the footnote. Parts of the manuscript used X to denote 10, but we have not followed that abbreviation in this version.- wdj]

x	x^2	$1/x$	$-x$
1	1	1	100
2	4	51	99
3	9	34	98
4	16	76	97
5	25	81	96
6	36	17	95
7	49	29	94
8	64	38	93
9	81	45	92
10	100	91	91
11	20	46	90
12	43	59	89
13	68	70	88
14	95	65	87
15	23	27	86
16	54	19	85
17	87	6	84
18	21	73	83
19	58	16	82
20	97	96	81
21	37	77	80
22	80	23	79
23	24	22	78
24	71	80	77
25	19	97	76
26	70	35	75
27	22	15	74
28	77	83	73
29	33	7	72
30	92	64	71
31	52	88	70
32	14	60	69
33	79	49	68
34	45	3	67
35	13	26	66
36	84	87	65
37	56	71	64
38	30	8	63
39	6	57	62
40	85	48	61
41	65	69	60
42	47	89	59
43	31	47	58
44	17	62	57
45	5	9	56
46	96	11	55
47	88	43	54
48	82	40	53
49	78	33	52
50	76	99	51
51	76	2	50
52	78	68	49
53	82	61	48
54	88	58	47
55	96	90	46
56	5	92	45
57	17	39	44
58	31	54	43
59	47	12	42
60	65	32	41
61	85	53	40
62	6	44	39
63	30	93	38
64	56	30	37
65	84	14	36
66	13	75	35
67	45	98	34
68	79	52	33
69	14	41	32
70	52	13	31
71	92	37	30
72	33	94	29
73	77	18	28
74	22	86	27
75	70	66	26
76	19	4	25
77	71	21	24
78	24	79	23
79	80	78	22
80	37	24	21
81	97	5	20
82	58	85	19
83	21	28	18
84	87	95	17
85	54	82	16
86	23	74	15
87	95	36	14
88	68	31	13
89	43	42	12
90	20	55	11
91	100	10	10
92	81	56	9
93	64	63	8
94	49	72	7
95	36	84	6
96	25	20	5
97	16	25	4
98	9	67	3
99	4	50	2
100	1	100	1

Table 1: Squares, reciprocals, negatives

and the fractions are quickly evaluated. Thus: $-79/36 = 96$ [*some details omitted - wdj*]. Determining the fractions in this manner, we write the two equations in the form:

$$x + 96y = 80, \qquad x + 29y = 37,$$

whence $y = 73$ and $x = 41$ [*some details omitted - wdj*].

The modulus 101 is very convenient to work with. The residue, modulo 101, of any integer is immediately obvious, at sight of the integer, and is therefore obtained without computation.

13 Reference matrices and table

We now turn our attention to the construction of reference matrices for checking in the field F_{101}. Our object is merely to give an account of problems arising. Hence the purposes of this paper will be served if we choose small illustrative matrices.

With

$$\begin{gathered} a_1 = 3,\ a_2 = 4,\ a_3 = 5,\ a_4 = 6,\ a_5 = 8, \\ a_6 = 25,\ a_7 = 35,\ a_8 = 15,\ a_9 = 42,\ a_{10} = 1, \end{gathered} \tag{6}$$

consider the reference matrix:

$$A = \begin{pmatrix} a_1 & a_2 & \dots & a_{10} \\ a_1^2 & a_2^2 & \dots & a_{10}^2 \\ \vdots & & & \vdots \\ a_1^5 & a_2^5 & \dots & a_{10}^5 \end{pmatrix} = \begin{pmatrix} 3 & 4 & 5 & 6 & 8 & 25 & 35 & 15 & 42 & 1 \\ 9 & 16 & 25 & 36 & 64 & 19 & 13 & 23 & 47 & 1 \\ 27 & 64 & 24 & 14 & 7 & 71 & 51 & 42 & 55 & 1 \\ 81 & 54 & 19 & 84 & 56 & 58 & 68 & 24 & 88 & 1 \\ 41 & 14 & 95 & 100 & 44 & 36 & 57 & 57 & 60 & 1 \end{pmatrix}$$

A q-element check, $q \leq 5$, on the sequence $f_1, f_2, \dots, f_n$ of n elements in F_{101}, $n \leq 10$, is given by

$$c_j = \sum_{i=1}^{n} a_i^j f_i, \qquad (j = 1, 2, \dots, q).$$

This check, being based upon the matrix A, will be called a check of "type A".

With

$$b_1 = 3,\ b_2 = 4,\ b_3 = 5,\ b_4 = 6,\ b_5 = 8,$$
$$b_6 = 25,\ b_7 = 35,\ b_8 = 1,$$

consider the matrix:

$$B = \begin{pmatrix} b_1 & b_2 & \dots & b_8 \\ b_1^2 & b_2^2 & \dots & b_8^2 \\ \vdots & & & \vdots \\ b_1^5 & b_2^5 & \dots & b_8^5 \end{pmatrix} = \begin{pmatrix} 3 & 4 & 5 & 6 & 8 & 25 & 35 & 1 \\ 9 & 16 & 25 & 36 & 64 & 19 & 13 & 1 \\ 27 & 64 & 24 & 14 & 7 & 71 & 51 & 1 \\ 81 & 54 & 19 & 84 & 56 & 58 & 68 & 1 \\ 41 & 14 & 95 & 100 & 44 & 36 & 57 & 1 \end{pmatrix}$$

which is evidently a submatrix of A. We can obtain a q-element check, $q \leq 5$, on the sequence $f_1, f_2, \dots, f_n$, $n \leq 8$, taking

$$c_j = \sum_{i=1}^{n} b_i^j f_i, \qquad (j = 1, 2, \dots, q).$$

This check will be called a check of "type B", since it is based upon the matrix B.

Table 2 enables us to evaluate easily the checks of types A and B. Table 2 contains nine rows of one hundred columns each[7]. The ith row shows the products of all non-zero elements of F_{101} by a_i $(i = 1, 2, \dots, 9)$, where the a_i's are given in equation (6).

Table 2 can be replaced by a highly convenient mechanical device, which greatly facilitates the rapid determination of the c_j's. But we are here only concerned with the mathematical description of checking operations, and not with devices to affect their practical application.

14 Illustration of checking in the field F_{101}

We wish to provide checks upon arbitrary sequences $f_1, f_2, \dots, f_n$ of elements of any given finite algebraic field. Operations in the field F_{101} can be used to illustrate all the essential points arising in this connection.

[7]I have omitted all but the first 14 columns, for brevity. - wdj

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	3	6	9	12	15	18	21	24	27	30	33	36	39	42
2	4	8	12	16	20	24	28	32	36	40	44	48	52	56
3	5	10	15	20	25	30	35	40	45	50	55	60	65	70
4	6	12	18	24	30	36	42	48	54	60	66	72	78	84
5	8	16	24	32	40	48	56	64	72	80	88	96	3	11
6	25	50	75	100	24	49	74	99	23	48	73	98	22	47
7	35	70	4	39	74	8	43	78	12	47	82	16	51	86
8	15	30	45	60	75	90	4	19	34	49	64	79	94	8
9	42	84	25	67	8	50	92	33	75	16	58	100	41	83

Table 2: A table of products with the a_i's.

Example 13 Check of Type A upon a sequence f_1, f_2, ..., f_{10}. Suppose that we wish, in a certain message, to transmit the numerical sequence

$$38460000600800000299.$$

The origin and significance of this sequence in the following form, in which it appears as a sequence of ten elements of F_{101}:

38	46	00	00	60	08	00	00	02	99
f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}

A five-element check ($q = 5$) is obtained by the simple tabulation which follows. We use Table 2, noting that in each of the nine rows, the one-hundred columns are shown in four sections, there being twenty-five columns in each section.

For the first element, 38, in the operand sequence f_i, place ruler under the proper section of row 1 of the Table. In row 1, read: 13 in column 38, 39 in column 13, 16 in column 39, 48 in column 16, 43 in column 48. Start a tabulation:

$$13 \quad 39 \quad 16 \quad 48 \quad 43.$$

For the second element, 46, in the operand sequence, place ruler under the proper section of row 2 of the Table. In row 2, read: 83 in column 46, 29 in column 83, 15 in column 29, 60 in column 15, 38 in column 60. Continue the tabulation:

13 39 16 48 4383 29 15 60 38

Since the third and fourth elements of the operand sequence are equal to zero, skip them entirely. For the fifth element, 60, read in row 5 of the Table: 76 in column 60, 2 in column 76, 16 in column 2, 27 in column 16, 14 in column 27. Continue the tabulation:

13 39 16 48 4383 29 15 60 3876 2 16 27 14

Proceed in this manner to the ninth element, 2, inclusive of the operand sequence. There being no tenth row in the Table, simply add the tenth element, 99, of the operand sequence in each vertical column of the tabulation. The full tabulation is:

13	39	16	48	43	
83	29	15	60	38	
76	2	16	27	14	
99	51	63	60	86	
84	94	9	75	19	
454	314	218	369	299	sum in $\mathbb{Z}$
50	11	16	66	97	sum in F_{101}

The five-element check is therefore:

$$c_1 = 50, c_2 = 11, c_3 = 16, c_4 = 66, c_5 = 97.$$

We transmit telegraphically the sequence of fifteen elements of F_{101}:

38 46 00 00 60 08 00 00 02 99 50 11 16 66 97.

A discussion of possible errors will be given in another section. we simply note here that the c_j's, as determined in the above tabulation, are:

$$c_1 = \sum_{i=1}^{10} a_i f_i, \quad c_2 = \sum_{i=1}^{10} a_i^2 f_i, \quad \ldots, c_5 = \sum_{i=1}^{10} a_i^5 f_i.$$

If only a one-element check had been desired, we should have taken $c_1 = 50$, and a one-column tabulation would have sufficed. If a two-element check

had been desired, we should have taken $c_1 = 50$, $c_2 = 11$ and a two-column tabulation would have sufficed. Etc.

If the operand sequence f_i contains less than 10 elements, the procedure, to determine check of Type A, is obvious. A q-element check upon f_1, f_2, ..., f_n, with $n < 10$, is as stated:

$$c_j = \sum_{i=1}^{10} a_i^j f_i, \qquad j = 1, 2, \ldots, q,$$

with $q = 1, 2, 3, 4, 5$. The manner of its evaluation, by means of Table 2, is clear.

Example 14 Check of Type B upon a sequence f_1, f_2, ..., f_8.

Suppose that we desire a five-element check upon the numerical sequence 6500000000001794 - that is, upon

65	00	00	00	00	00	17	94
f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8

We wish to evaluate $c_j = \sum_{i=1}^{8} b_i^j f_i$, $\qquad (j = 1, 2, \ldots, 5)$. The tabulation is as follows:

94	80	38	13	39	row 1, Table 2, read: 94 in col. 65, etc.
90	19	59	45	60	row 7, read: 90 in col. 17, etc.
94	94	94	94	94	
278	193	191	152	193	sum in $\mathbb{Z}$
76	92	90	51	92	sum in F_{101}
c_1	c_2	c_3	c_4	c_5	

Example 15 Check of Type A upon the same operand sequence as in Example 14.

We wish to evaluate $c_j = \sum_{i=1}^{8} a_i^j f_i$, $\qquad (j = 1, 2, \ldots, 5)$. The tabulation is as follows:

94	80	38	13	39	
90	19	59	45	60	
97	41	9	34	5	row 8, Table 2, read: 97 in col. 94, etc.
281	140	106	92	104	sum in $\mathbb{Z}$
79	39	5	92	3	sum in F_{101}
c_1	c_2	c_3	c_4	c_5	

Example 16 Check of Type A and B upon the operand sequence

00	65	00	00	00	17	94
f_1	f_2	f_3	f_4	f_5	f_6	f_7

We wish to evaluate

$$c_j = \sum_{i=1}^{7} a_i^j f_i = \sum_{i=1}^{7} b_i^j f_i, \qquad (j = 1, 2, \ldots, 5).$$

The tabulation is as follows:

58	30	19	76	1	row 2, Table 2, read: 58 in col. 65, etc.
21	20	96	77	6	row 6, read: 21 in col. 17, etc.
58	10	47	29	5	row 7, read: 58 in col. 94, etc.
137	60	162	182	12	sum in $\mathbb{Z}$
36	60	61	81	12	sum in F_{101}
c_1	c_2	c_3	c_4	c_5	

Questions of rigor will be discussed in a subsequent section. It may be noted here, however, that our checks make very nice discriminations. Thus, although the operand sequence in Examples 15 and 16 are closely similar, the checking sequences are widely different.

It will now be apparent to those who are acquainted with the problems of code communication that we are in a position to furnish powerful and economical checks on message sequences in any conceivable telegraphic system. We have only to partition messages into groups of not more than ten, or not more that eight, elements each – according to any definite prearrangement – and to check each group with a q-check, $q = 1, 2, 3, 4, 5$ (as may be arranged), of Type A or of Type B. If it is desired to work with longer groups, we have only to enlarge Table 2. The limitations introduced in this paper may be largely overcome, or removed, by suitable amplification of the Table employed.

15 Lemma concerning reference matrices

The general reference matrix of section 3 was:

$$Q = \begin{pmatrix} k_{11} & k_{12} & \dots & k_{1n} \\ k_{21} & k_{22} & \dots & k_{2n} \\ \vdots & & & \vdots \\ k_{q1} & k_{q2} & \dots & k_{qn} \end{pmatrix}$$

the k_{ij} being elements of any given finite algebraic field F, and q being less than or equal to n.

This matrix contains determinants of order r with $r = 1, 2, \dots, q$ – determinants of first order ($r = 1$) being single elements of the matrix.

We recall that if f_1, f_2, ..., f_s is an s element operand sequence in F, a t-element check based upon the matrix Q is:

$$c_j = \sum_{i=1}^{s} k_{ji} f_i, \qquad (j = 1, 2, \dots, t).$$

it being understood that $s \leq n$, $t \leq q$.

Let Q contain no vanishing determinant of any order: Let c_1, c_2, ..., c_t be a t-element check, $t \leq q$, on the operand sequence f_1, f_2, ..., f_s, $s \leq n$. Let v be a positive integer less than or equal to $s + t$. If, in the transmittal of the sequence

$$f_1, f_2, \dots, f_s, c_1, c_2, \dots, c_t,$$

errors occur in v of its $s+t$ elements, *whatever the distribution of the errors*, the presence of error will certainly be disclosed, or will enjoy only a 1-in-$(\Gamma - 1)^t$ chance of escaping disclosure, according as v is, or is not, less than $t + 1$. In this statement, Γ denotes the total number of elements in the field F.

proof:

Case 1 Let all v errors fall among the $c_1, c_2, \dots, c_t$. The presence of error is evidently certain to be disclosed.

Case 2 Let all v errors fall among the $f_1, f_2, \dots, f_s$.

(2.1): Let $v \leq t$. There is no loss of generality of we assume[8] the v errors are ϵ_1, ϵ_2, ..., ϵ_v, affecting $f_1, f_2, \dots, f_v$. The errors cannot

[8]This assumption implies $v \leq s$. - wdj

escape disclosure. For, to do so, they would have to satisfy the system of homogeneous linear equations:

$$\sum_{i=1}^{v} k_{ji}\epsilon_i, \qquad (j = 1, 2, \ldots, t).$$

in which the matrix of coefficients k_{ji} contains no vanishing determinant of any order, and which, therefore admits no solution other than $\epsilon_i = 0$ $(i = 1, 2, \ldots, v)$.

For this treatment of the errors, compare Sections 4, 5.

(2.2): Let $v > t$. Compare the theorem given at the close of Section 5.

Case 3 Let z errors fall among the f_i and $w = v - z$ errors fall among the c_j. Without loss in generality, we may assume that the errors are ϵ_1, ϵ_2, $\ldots$, ϵ_z, affecting $f_1, f_2, \ldots, f_z$, and δ_{j_1}, δ_{j_2}, $\ldots$, δ_{j_w}, affecting c_{j_1}, c_{j_2}, $\ldots$, c_{j_w}.

(3.1): Let $z + w \leq t$. Writing $t = v + h = z + w + h$, where h denotes a non-negative integer which may or may not be zero, we have $t - w = z + h$. Hence $z + h$ of the c_j are transmitted without error.

If the presence of error is to escape disclosure, we see, therefore, that the z errors ϵ_i must satisfy the system of at least z homogeneous linear equations:

$$\sum_{i=1}^{z} k_{r_m,i}\epsilon_i, \qquad (m = 1, 2, \ldots, z + h),$$

where the indices r_m denote a set of $z + h$ integers selected from $1, 2, \ldots, t$. But the matrix of coefficients in this system contains no vanishing determinant, so that the only solution would be $\epsilon_i = 0$ $(i = 1, 2, \ldots, z)$.

For details in this treatment of errors, see Section 5.

(3.2): Let $z + w > t$. Then $w = t - (z - h)$, where h denotes a positive integer. Assuming that the presence of error is to escape detection, we see, therefore, that the v errors must satisfy t linear equations as follows:

(α) a system of $z - h$ equations involving only the errors ϵ_i, ($i = 1, 2, \ldots, z$), and homogeneous in these z errors;

(β) a system of w equations involving all v errors.

Since the matrix of the coefficients in the system (α) contains no vamishing determinant, we can solve this system for $z - h$ of the ϵ_i as rational functions of the remaining h of the ϵ_i.

The system (β) determines all errors affecting the c_j – that is, all the errors δ_{j_i} – as polynomial functions of the ϵ_i, ($i = 1, 2, \ldots, z$).

Hence, all told, $(z - h) + w$ errors are determined as rational functions of the remaining h errors. In other words, $v - t$ errors determine the other t errors.

An accidental error can assume any one of $\Gamma - 1$ values, there being Γ elements in the finite field F. Hence the chance that the errors will check up, and thus escape disclosure, is only 1-in-$(\Gamma - 1)^t$. QED

16 Checks based upon Table 2: strength of checks of type A

Referring to the matrix A of type A checks (section 14), let us consider the submatrix

$$A' = \begin{pmatrix} a_1 & a_2 & \ldots & a_{10} \\ a_1^2 & a_2^2 & \ldots & a_{10}^2 \\ a_1^3 & a_2^3 & \ldots & a_{10}^3 \\ a_1^4 & a_2^4 & \ldots & a_{10}^4 \end{pmatrix}.$$

We shall now show that the matrix A' contains no vanishing determinant of any order. We might easily built up a matrix A with this property. But it seemed advisable to make a discussion along general lines, pointing out thereby the problem arising in the analysis of any reference matrix.

1. By the argument of Section 7, we may show at once that A' contains no vanishing determinant of the fourth order.

2. Determinants of the third order in A' are of the four types

$$(a^2, a^3, a^4), \quad (a, a^3, a^4), \quad (a, a^2, a^4), \quad (a, a^2, a^3),$$

where (a^r, a^s, a^t) denotes the determinant

$$\begin{vmatrix} a^r & b^r & c^r \\ a^s & b^s & c^s \\ a^t & b^t & c^t \end{vmatrix},$$

and a, b, c denote three different a_i $(i = 1, 2, \ldots, 10)$.

(2.1) We have: $(a^2, a^3, a^4) = abc(a, a^2, a^3)$; that is to say:

$$\begin{vmatrix} a^2 & b^2 & c^2 \\ a^3 & b^3 & c^3 \\ a^4 & b^4 & c^4 \end{vmatrix} = abc \begin{vmatrix} a & b & c \\ a^2 & b^2 & c^2 \\ a^3 & b^3 & c^3 \end{vmatrix}.$$

This, since a, b, c are all different from the zero element of F_{101}, the determinants (a^2, a^3, a^4) and (a, a^2, a^3) vanish simultaneously.

If we had $(a, a^2, a^3) = 0$ then a, b, c would be roots of an algebraic equation of the third degree $ux + vx^2 + wx^3 = 0$ with coefficients u, v, w lying in F_{101} and not all zero (cf, Lemma 4, Section 2). Since $x = 0$ is manifest a root of this equation, the equation would have four different roots, contrary to Lemma 5.

(2.2) Consider $(a, a^3, a^4) = abc(a^0, a^2, a^3)$.

If

$$\begin{vmatrix} 1 & 1 & 1 \\ a^3 & b^3 & c^3 \\ a^4 & b^4 & c^4 \end{vmatrix} = 0,$$

there is an algebraic equation of the third degree[9] $ux + vx^2 + wx^3 = 0$ with coefficients u, v, w lying in F_{101} and not all zero, which has a, b, c as roots. Then, by the relations between the coefficients of an algebraic equation and symmetric functions of its roots – relations valid in any field – we must have:

[9]If F is any algebraic field and λ denotes any element, other than the zero element, of F then, as is known to the reader, λ^0 denotes the unit element of F.

$$ab + bc + ca = 0.$$

By the a_i, in the matrix A', have been selected so that this condition is never satisfied.

(2.3) In a like manner, we have $(a, a^2, a^4) = abc(a^0, a, a^3)$; and we really show that if

$$(a^0, a, a^3) = \begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^3 & b^3 & c^3 \end{vmatrix} = 0,$$

we must have: $a + b + c = 0$. But the a_i have been selected so that this condition is never satisfied.

Hence no third-order determinant of A' vanishes.

3. It is easily shown that no second-order determinant of A' vanishes. For, if a, b are any two different a_i, we find that $a^2 = b^2$. And, moreover, if a, b are any two different elements of the field F_{101}, we easily show that $a^3 \neq b^3$. The last statement may be proved by an argument similar to that employed at the close of Section 8. It brings out an important advantage, as far as our checking is concerned, which the field F_{101} possesses over the field F_{97} – a field related to the prime 97 precisely as F_{101} is related to the prime 101.

4. Evidently, no single element of A' vanishes. Hence A' contains no vanishes determinant of the first order.

A' contains, as was to be shown, not vanishing determinant of any order.

It follows, by Section 15, that when a q-element check $(c, c_2, \ldots, c_q)$ of type A, with $q \leq 4$, is transmitted with the operand sequnece $f_1, f_2, \ldots, f_n$, $n \leq 10$, the amplified sequence under actual transmittal thus being: (S) $f_1, f_2, \ldots, f_n, c, c_2, \ldots, c_q$ $(n \leq 10,\ q \leq 4)$, the following statement can be made: If errors occur in v of the $n + q$ elements of (S), the presence of error will infallibly be disclosed, or will enjoy a

$$1 - in - 100^q$$

chance of escaping disclosure, according as v is, or is not, less than $q + 1$.

Example 17 Referring to Example 13, Section 14, suppose that we transmit the operand sequence

$$38\ \ 46\ \ 00\ \ 00\ \ 60\ \ 08\ \ 00\ \ 00\ \ 02\ \ 99:$$

(α) with a four-element check, thus:

$$38\ \ 46\ \ 00\ \ 00\ \ 60\ \ 08\ \ 00\ \ 00\ \ 02\ \ 99\ \ 50\ \ 11\ \ 16\ \ 66$$

(β) with a three-element check, thus:

$$38\ \ 46\ \ 00\ \ 00\ \ 60\ \ 08\ \ 00\ \ 00\ \ 02\ \ 99\ \ 50\ \ 11\ \ 16$$

(γ) with a two-element check, thus:

$$38\ \ 46\ \ 00\ \ 00\ \ 60\ \ 08\ \ 00\ \ 00\ \ 02\ \ 99\ \ 50\ \ 11$$

(δ) with a one-element check, thus:

$$38\ \ 46\ \ 00\ \ 00\ \ 60\ \ 08\ \ 00\ \ 00\ \ 02\ \ 99\ \ 50$$

In case (α), any distribution of less than or equal than five errors among the fifteen elements of the sequence will certainly be disclosed; any distribution of five of more errors will not enjoy better than a

$$1 - in - 100000000$$

chance of escaping disclosure.

In case (β), any distribution of less than or equal than four errors among the fifteen elements of the sequence will certainly be disclosed; any distribution of four of more errors will not enjoy better than a

$$1 - in - 1000000$$

chance of escaping disclosure.

Etc.

17 Checks based upon table 4: strength of checks of type B

The matrix B of type B checks, section 13, contains no vanishing determinant of any order.

1. There is no vanishing determinant of the fifth order, as shown in Section 7.

2. Determinants of the fourth order are of the types:

   $$(a^2, a^3, a^4, a^5),\ \ (a, a^3, a^4, a^5),\ \ (a, a^2, a^4, a^5),\ \ (a, a^2, a^3, a^5),\ \ (a, a^2, a^3, a^4),$$

   where (a^p, a^r, a^s, a^t) denotes the determinant

   $$\begin{vmatrix} a^p & b^p & c^p & d^p \\ a^r & b^r & c^r & d^r \\ a^s & b^s & c^s & d^s \\ a^t & b^t & c^t & d^t \end{vmatrix},$$

   and a, b, c, d denote four different b_i $(i = 1, 2, \ldots, 8)$.

   (2.1) The first and fifth types vanish simultaneously. But if we had $(a, a^2, a^3, a^4) = 0$, as we should have, in F_{101}, a fourth-degree algebraic equation with five distinct roots (one of which would be $x = 0$). By Lemma 5, this is inadmissible.

   (2.2) Let $(a, a^3, a^4, a^5) = 0$. Then, since a, b, c, d are all different from the zero element of F_{101}, we have: $(a^0, a^2, a^3, a^4) = 0$. Hence, a, b, c, d would be roots of an algebraic equation of the fourth degree

   $$t + ux^2 + vx^3 + wx^4 = 0,$$

   with coefficients t, u, v, w lying in F_{101} and not all zero (cf, Lemma 4, Section 2). We must therefore have:

   $$abc + abd + acd + bcd = 0,$$

   a relation which is excluded by our selection of the b_i $(i = 1, 2, \ldots, 8)$.

(2.3) In like manner it is easy to argue that $(a, a^2, a^4, a^5) = 0$ would imply the relation

$$ab + ac + ad + bc + bd + cd = 0,$$

and that $(a, a^2, a^3, a^5) = 0$ would imply the relation

$$a + b + c + d = 0,$$

both of these relations, however, being excluded by our selection of the b_i.

Hence B contains no vanishing determinant of the fourth order.

(2.3) There are ten types of third order determinants in B. But the treatment for all but three of these has already been considered. The three remaining are:

(α)
$$\begin{vmatrix} a & b & c \\ a^4 & b^4 & c^4 \\ a^5 & b^5 & c^5 \end{vmatrix} = abc \begin{vmatrix} 1 & 1 & 1 \\ a^3 & b^3 & c^3 \\ a^4 & b^4 & c^4 \end{vmatrix},$$

(β)
$$\begin{vmatrix} a & b & c \\ a^3 & b^3 & c^3 \\ a^5 & b^5 & c^5 \end{vmatrix} = abc \begin{vmatrix} 1 & 1 & 1 \\ a^2 & b^2 & c^2 \\ a^4 & b^4 & c^4 \end{vmatrix},$$

(γ)
$$\begin{vmatrix} a & b & c \\ a^2 & b^2 & c^2 \\ a^5 & b^5 & c^5 \end{vmatrix} = abc \begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^4 & b^4 & c^4 \end{vmatrix},$$

where a, b, c are three different b_i $(i = 1, 2, \ldots, 8)$.

3. (3.1) Suppose that we have:

$$\begin{vmatrix} 1 & 1 & 1 \\ a^2 & b^2 & c^2 \\ a^4 & b^4 & c^4 \end{vmatrix} = 0.$$

Then a, b, c are three roots of an algebraic equation of the fourth degree

$$u + vx^3 + wx^4 = 0,$$

with coefficients u, v, w lying in F_{101} and not all zero (cf, Lemma 4, Section 2).

Let the fourth root of this equation, not necessarily distinct from a, b, c, be called Λ. Then we have two relations:

$$ab + ac + a\lambda + bc + b\lambda + c\lambda = 0, \quad abc + ab\lambda + bc + ac\lambda + bc\lambda = 0,$$

from which we conclude that:

$$(ab + bc + ca)^2 = abc(a + b + c).$$

The selection of the b_i $(i = 1, 2, \ldots, 8)$ guarantees that this last relation is never satisfied.

(3.2) The determinant

$$\begin{vmatrix} 1 & 1 & 1 \\ a^2 & b^2 & c^2 \\ a^4 & b^4 & c^4 \end{vmatrix}$$

is of the same type as

$$\begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{vmatrix}$$

(cf, the case 4 below) and therefore, as already pointed out, cannot vanish.

(3.3) It is really argued that the vanishing of

$$\begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^4 & b^4 & c^4 \end{vmatrix}$$

would imply the relation

$$(a + b + c)^2 = ab + bc + ca;$$

and this relation is excluded by our choice of the b_i $(i = 1, 2, \ldots, 8)$

Hence B contains no vanishing determinant of the third order.

4. We have already seen that if a, b are two different a_i we may write $a^2 \neq b^2$, $a^3 \neq b^3$. These relations hold, a fortiori, if a, b are two different b_i. Moreover, the b_i have been choosen so that if a, b are two different b_i, we may write $a^4 \neq b^4$. It is therefore clear that B contains no vanishing determinant of the second order.

B contains no vanishing determinant of any order.

It follows, by Section 15, that when a q-element check $(c, c_2, \ldots, c_q)$ of type B, with $q \leq 5$, is transmitted with the operand sequnece $f_1, f_2, \ldots, f_n$, $n \leq 8$, the amplified sequence under actual transmittal thus being: (S) $f_1, f_2, \ldots, f_n, c, c_2, \ldots, c_q$ $(n \leq 8,\ q \leq 5)$, the following statement can be made[10]: If errors occur in v of the $n+q$ elements of (S), the presence of error will infallibly be disclosed, or will enjoy a

$$1 - in - 100^q$$

chance of escaping disclosure, according as v is, or is not, less than $q + 1$.

Example 18 Referring to Example 13, Section 14, suppose that we transmit the operand sequence

$$65 \quad 00 \quad 00 \quad 00 \quad 00 \quad 00 \quad 17 \quad 94$$

is transmitted with the five-element check of type B

$$76 \quad 92 \quad 90 \quad 51 \quad 92,$$

any distribution of less than six errors among the thirteen elements of the amplified sequence

$$65 \quad 00 \quad 00 \quad 00 \quad 00 \quad 00 \quad 17 \quad 94 \quad 76 \quad 92 \quad 90 \quad 51 \quad 92$$

is bound to be disclosed; any distribution of four of more errors will not enjoy better than a

$$1 - in - 10000000000$$

chance of escaping disclosure.

[10]Compare the corresponding statement for checks of type A (Section 16).

18 Comment upon matrix A

The matrix A, section 13, the basis of full five-element checks upon operand sequeces with as many as ten elements, does contain vanishing determinants. We purposely arranged it so that this would be the case, and an opportunity provided for a complete discussion of important points.

We know that:

$$\begin{vmatrix} a_1 & a_5 & a_8 \\ a_1^4 & a_5^4 & a_8^4 \\ a_1^5 & a_5^5 & a_8^5 \end{vmatrix} = 0.$$

where $a_1 = 3$, $a_5 = 8$, $a_8 = 15$, $a_9 = 42$.

To appreciate the influence of these vanishing determinants, let us review the operand-and-checking sequence of Example 13, Section 14:

38	46	00	00	60	08	00	00	02	99	50	11	16	66	97
f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	c_1	c_2	c_3	c_4	c_5

The anomalous situation prevailing may be expressed in the statement: If exactly 5 errors occur, and in precisely one of the particular distributions:

(a) f_1, f_5, f_8, c_2, c_3,

(b) f_1, f_5, f_9, c_3, c_4,

the presence of error, instead of being certain of disclosure, will enjoy a 1–in–100000000 chance of escaping disclosure.

Consider, for example, the case (a). Let the five errors

$$\epsilon_1, \epsilon_5, \epsilon_8, \delta_2, \delta_3,$$

be made respectively in the elements f_1, f_5, f_8, c_2, c_3 of the sequence.

If these errors are to escape disclosure, they must satisfy the three homogeneous linear equations:

$$3\epsilon_1 + 8\epsilon_5 + 15\epsilon_8 = 0,$$
$$3^4\epsilon_1 + 8^4\epsilon_5 + 15^4\epsilon_8 = 0,$$
$$3^5\epsilon_1 + 8^5\epsilon_5 + 15^5\epsilon_8 = 0,$$

and also the two equations

$$3^2\epsilon_1 + 8^2\epsilon_5 + 15^2\epsilon_8 = \delta_2,$$
$$3^3\epsilon_1 + 8^3\epsilon_5 + 15^3\epsilon_8 = \delta_3.$$

The homogeneous system may be written

$$3\epsilon_1 + 8\epsilon_5 + 15\epsilon_8 = 0,$$
$$81\epsilon_1 + 56\epsilon_5 + 24\epsilon_8 = 0,$$
$$41\epsilon_1 + 44\epsilon_5 + 57\epsilon_8 = 0,$$

and is found to have the solution

$$\epsilon_5 = 81\epsilon_1, \epsilon_8 = 98\epsilon_1.$$

Then the other two equations determine δ_2 and δ_3 as follows

$$\delta_2 = 9\epsilon_1 + 64\epsilon_5 + 23\epsilon_8 = 74\epsilon_1,$$
$$\delta_3 = 27\epsilon_1 + 7\epsilon_5 + 42\epsilon_8 = 64\epsilon_1.$$

We may choose the value of ϵ_1 arbitrarily. But the values of the other four errors are then fixed.

Thus, if f_1 is erroneously transmitted as 88 instead of 38, so that $\epsilon_1 = 88 - 38 = 50$, we obtain: $\epsilon_5 = 10$, $\epsilon_8 = 52$, $\delta_2 = 64$, $\delta_3 = 69$.

If, therefore, we alter the five elements f_1, f_5, f_8, c_2, c_3 of the sequence as follows:

$$f_1' = f_1 + \epsilon_1 = f_1 + 50 = 88, f_5' = f_5 + \epsilon_5 = 70, f_8' = f_8 + \epsilon_8 = 52,$$
$$c_2' = c_2 + \delta_2 = 75, c_3' = c_3 + \delta_3 = 85,$$

the resulting sequence

88	46	00	00	70	08	00	52	02	99	50	75	85	66	97
f_1'	f_2	f_3	f_4	f_5'	f_6	f_7	f_8'	f_9	f_{10}	c_1	c_2'	c_3'	c_4	c_5

is in full five-element check. In fact, the tabulation to obtain a five-element check of type A upon the operation sequence

88 46 00 00 70 08 00 52 02 99

is as follows:

62	85	53	58	73	
83	29	15	60	38	
55	36	86	82	50	... reading in 5th row, Table 2
99	51	63	60	86	
73	85	63	36	35	... reading in 8th row, Table 2
84	94	9	75	19	
99	99	99	99	99	
555	479	388	470	400	
50	75	85	66	97	

The advantage of working with reference matrices which contain no vanishing determinant of any order is now fully evident.

19 Conclusion

Further problems connected with checking operations in finite fields will be treated in another paper.

Machines may be devised to render almost quite automatic the evaluation of checking elements $c_1, c_2, \ldots, c_q$ according to any proposed reference matrix of the general type described in Section 7, whatever the finite field in which the operations are effected. Such machines would enable us to dispense entirely with tables of any sort, and checks could be determined with great speed. But before checking machines could be seriously planned, the following problem – which is one, incidentally, of considerable interest from the standpoint of pure number theory – would require solution:

To construct, for a given finite field F with Γ elements, and for the checking therein of n-element sequence $f_1, f_2, \ldots, f_n$, a reference matrix

$$\begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ a_1^2 & a_2^2 & \ldots & a_n^2 \\ \vdots & & & \vdots \\ a_1^q & a_2^q & \ldots & a_n^q \end{pmatrix}$$

without a vanishing determinant of any order, in which the integer q is the greatest possible. Corresponding to any F, and any n – provided that n is less than Γ *– there is a definite maximum q. this maximum can you should be ascertained, and the reference matrix therefore constructed.*

We are not able to communicate a solution of this general problem.

(signed) Lester S. Hill

References

[D] L. E. Dickson, **Linear groups with an exposition of the Galois field theory**, B. G. Teubner, Leipzig, 1901. Available here: `http://archive.org/details/lineargroupswith00dickuoft`

[H1] Lester R. Hill, *A novel checking method for telegraphic sequences,* Telegraph and Telephone Age (October 1, 1926), 456 - 460.

[H2] ——, *The role of prime numbers in the checking of telegraphic communications, I* Telegraph and Telephone Age (April 1, 1927), 151 - 154.

[H3] ——, *The role of prime numbers in the checking of telegraphic communications, II* Telegraph and Telephone Age (July, 16, 1927), 323 - 324.

[Sc] G. Scorza, **Corpi numerici e algebre**, Giuseppe Principato, 1921.

[St] E. Steinitz, *Algebraische theorie der körper*, Journal für die reine und angew. Mathamtik 137(1910)167-308.