STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1951 - 012

Coding problems in the theory of computing machines

H.J.A. Duparc

1951

Coding problems in the theory of computing machines.

by H.J.A. Duparc.

§ 1. Coding.

In the computing machines we are to consider in this theory every decimal digit x of a number a will be given in code. The digit x will be identified with a set of n numbers $x_1,\ldots,x_n$ which we shall call the coordinates of the digit x. We write $x = (x_1,\ldots,x_n)$.

We shall always take every $x_i = 1$ or 0, so that every digit x might be represented by the running or not running of a current through everyone of n conductors; the theory can, however, be extended to the case in which x_i can have more different values.

A simple example is known, where n = 4 and the 4 coordinates correspond with the representation of the number x in the binary system, i.e. 0 = (0,0,0,0); 1 = (0,0,0,1); 2 = (0,0,1,0); ...; 9 = (1,0,0,1). This, however, is by no means the only way in which the ten digits 0,1,...,9 can be coded by means of quadruples of coordinates, for there exist 16 such quadruples, and the number of ways in which we can select 10 of them to correspond with our digits, 0,1,...,9 is equal to $\frac{16!}{6!}$. The choice we did when adopting the binary representation possesses the property that for every x we have $x = 8x_1 + 4x_2 + 2x_3 + x_4$. The coefficients 8,4,2,1 which occur in this formula are called the weights of the coordinates in our representation. In § 5 we shall further concern this notion of weights.

We further remark that the choice n = 4 is not compulsory. If for instance n = 5 we have more freedom in fixing a codation for we have to make a choice out of $\frac{32!}{22!}$ possibilities and in general for every $n \geqslant 4$ a choice out of $\frac{2^n!}{(2^n-10)!}$ possibilities. If $n < 4$ no codation exists because there are only 2^n different n-ples of coordinates, which number is insufficient to indicate the 10 digits 0,1,...,9, since for $n < 4$ we have $2^n < 10$.

Suppose a codation has been chosen with $n \geqslant 4$. A number written in the decimal system in the form xyz... will be written in code if any of its digits is written in code. If the number possesses m decimal digits, it possesses mn coordinates $x_1,\ldots,x_n, y_1,\ldots,y_n, \ldots$ each of which has a value 0 or 1. If for instance we take n = 4 and adopt coordinates corresponding to the binary way of writing each digit, one has

$$34 = (0,0,1,1;\ 0,1,0,0); \qquad 64 = (0,1,1,0;\ 0,1,0,0).$$

Obviously the number of coordinates is larger than in the case the original number is entirely written in the binary system; the difference of the numbers of coordinates is due to the fact firstly that not necessarily the

smallest possible choice will be made for n and secondly that 10 is no integral power of 2.

§ 2. Operations with coded numbers.

If a way of coding is fixed, we want to find what operations on the coordinates of two numbers a and b have to be performed so as to obtain the coordinates of the sum, the difference, the product, ... of a and b.

We first have to restrict ourselves to the case $0 \leqq a \leqq 9$; $0 \leqq b \leqq 9$. The sum $S = a + b$ in this case only contains one or two digits, which we want to find from a and b. The number s of the units in S with $0 \leqq s \leqq 9$ possesses n coordinates s_ν each of which is a function of the 2n coordinates of a and b. One has

$$s_\nu = s_\nu(a_1,\ldots,a_n;\ b_1,\ldots,b_n) \qquad (\nu = 1,\ldots,n).$$

In the same way we see that the first digit t (which is called the "carry") of S is given by its coordinates:

$$t_\nu = t_\nu\ (a_1,\ldots,a_n;\ b_1,\ldots,b_n) \qquad (\nu = 1,\ldots,n).$$

As soon as the codation is fixed, so are the functions s_ν and t_ν of 2n integer variables, each of which is equal to 0 or 1. A single obvious property of these functions may be mentioned here. From $a + b = b + a$, one immediately finds for $\nu = 1,\ldots,n$

$$s_\nu\ (a_1,\ldots,a_n,\ b_1,\ldots,b_n) = s_\nu(b_1,\ldots,b_n,\ a_1,\ldots,a_n),$$
$$t_\nu\ (a_1,\ldots,a_n,\ b_1,\ldots,b_n) = t_\nu(b_1,\ldots,b_n,\ a_1,\ldots,a_n).$$

If addition formula are obtained for the sum $a + b$ with $0 \leqq a \leqq 9$; $0 \leqq b \leqq 9$ one finds immediately the way in which numbers a and b with more than one decimal digit must be added. For instance $v = xy + zu$, where x and y are the digits of the integer $10x + y$, and z, u of $10z + u$, is determined by 3n coordinates $v_1,\ldots,v_n;\ v_{n+1},\ldots,v_{2n};\ v_{2n+1},\ldots,v_{3n}$ with

$$v_{2n+\nu} = s_\nu\ (y_\mu;\ u_\mu)$$
$$v_{n+\nu} = s_\nu\ (t_\mu\ (y_\mu;\ u_\mu);\ \ s_\mu\ (x_{\mu'},\ z_{\mu'}))$$
$$v_\nu = s_\nu\ (t_\mu(x_\mu,\ z_\mu),\ t_\mu(t_{\mu'}(y_{\mu''},\ u_{\mu''});\ \ s_{\mu'}(x_{\mu'};\ z_{\mu''})));$$

here $\nu = 1,2,\ldots,n$ and x_μ is an abbreviation for $x_1,\ldots,x_n$; so are

$$x_{\mu'},\ x_{\mu''},\ y_{\mu'},\ y_{\mu''},\ z_\mu,\ z_{\mu'},\ z_{\mu''},\ s_\mu,\ s_{\mu'},\ t_\mu,\ t_{\mu'}.$$

Similar processes give us for two numbers a and b with $0 \leqq a \leqq 9$; $0 \leqq b \leqq 9$ the multiplication formulae

$$p_\nu = p_\nu\ (a_1,\ldots,a_n;\ b_1,\ldots,b_n) \qquad (\nu = 1,\ldots,n)$$
$$q_\nu = q_\nu\ (a_1,\ldots,a_n;\ b_1,\ldots,b_n) \qquad (\nu = 1,\ldots,n)$$

for the product $10\,p + q = ab$, and as soon as the functions p_ν and q_ν which furnish us with the multiplication of integers $\leqq 9$ are found, one is able to construct the coordinates of products in which the positive integer factors may be arbitrary. The formula for q_ν give us the carry,

which in the case of multiplication may represent all integer values $0,1,\ldots,8$, but not the value 9.

§3. Properties of functions mod 2.

The number of possible functions $f(x,y)$ which may only assume the values 0 or 1 for $x = 0$ or 1 and $y = 0$ or 1 is limited. In fact there exist but 16 such functions which we investigate now. If the scheme

y \ x	0	1
0	a	b
1	c	d

means $f(0,0) = a$; $f(0,1) = c$; $f(1,0) = b$; $f(1,1) = d$, one finds the following 8 possible formulae

y \ x	0	1
0	0	0;
1	0	0

y \ x	0	1
0	0	0;
1	0	1

y \ x	0	1
0	0	1
1	0	0

y \ x	0	1
0	0	0;
1	1	0

y \ x	0	1
0	1	0
1	0	0

y \ x	0	1
0	0	0
1	1	1

y \ x	0	1
0	0	1
1	0	1

y \ x	0	1
0	0	1
1	1	0

and the 8 other formulae which are derived from the above formulae by adding 1 (mod 2) to each of the values $f(x,y)$. These 16 formulae may be written in the form

$$f_1(x,y) = 0;\ f_2(x,y) = xy;\ f_3(x,y) = xy+x;\ f_4(x,y) = xy+y;$$

$$f_5(x,y) = xy+x+y;\ f_6(x,y) = y;\ f_7(x,y) = x;\ f_8(x,y) = x+y;$$

$$f_9(x,y) = 1;\ f_{10}(x,y) = xy+1;\ f_{11}(x,y) = xy+x+1;\ f_{12}(x,y) = xy+y+1;$$

$$f_{13}(x,y) = xy+x+y+1;\ f_{14}(x,y) = y+1;\ f_{15}(x,y) = x+1;\ f_{16} = x+y+1.$$

Further we remark that each of these formulae can be written in the form

$$f(x,y) = c_0 + c_1x + c_2y + c_3xy,$$

where the coefficients c_i are equal to 0 or 1.

This result which immediately can be verified from our 16 formulae may also be proved by making c_0, c_1, c_2, c_3 to satisfy to the four relations

$$f(0,0) = a;\ f(1,0) = b;\ f(0,1) = c;\ f(1,1) = d.$$

We then obtain four linear non homogeneous equations for c_0, c_1, c_2, c_3, where the determinant of the coefficients

$$\begin{vmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{vmatrix} = 1$$

is different from zero, whence it follows that these equations can be solved.

Consider now the more general case in which functions $f(x_1,\ldots,x_n)$

occur, where both any of the variables $x_1,\ldots,x_n$ and the function itself only take the value 0 or 1.

The number of different functions, which number was equal to 16 for $n = 2$, is now 2^{2^n}, since every x_ν may assume two values; so there are 2^n sets $(x_1,\ldots,x_n)$, and $f(x_1,\ldots,x_n)$ may be equal to 0 or 1 for everyone of those sets.

We now prove the fundamental

Theorem. Every function $f(x_1,\ldots,x_n)$, which together with each of the arguments $x_1,\ldots,x_n$ may assume only the value 0 or 1 and which for any arbitrary set $(x_1,\ldots,x_n)$ takes a prescribed value (which is either 0 or 1), can be written in the form

$$(1) \qquad f(x_1,\ldots,x_n) = \sum c_{\nu_1\nu_2\ldots\nu_k} x_{\nu_1} x_{\nu_2}\ldots x_{\nu_k}.$$

Here the sum is extended over all $k = 0,1,\ldots,n$ and, once k is chosen, over all possible choices of k of the n variables $x_1,\ldots,x_n$.

The theorem is proved if we show that coefficients c can be found so as to satisfy (1) and the conditions imposed on $f(x_1,\ldots,x_n)$. The number of coefficients c is equal to $\binom{n}{0}+\binom{n}{1}+\ldots+\binom{n}{n} = 2^n$ and these 2^n coefficients must satisfy any linear equation obtained by putting $f(x_1,\ldots,x_n)$ equal to the value it must assume for a given set $(x_1,\ldots,x_n)$. The number of the so obtained equations is at most equal to 2^n. If this number is less than 2^n we impose on f the extra condition to be equal to a number b for anyone of the sets $(x_1,\ldots,x_n)$ for which previously no prescribed value of f had been given. So in every case we obtain exactly 2^n linear equations in the 2^n unknown coefficients c. If this system can be solved so can the original set. We show that the extended system possesses exactly 1 solution. The original set then possesses at least one solution.

Consider first the relation $f(0,0,\ldots,0) = b_o$, from which we infer $c_o = b_o$. Next consider any of the equations $f(1,0,\ldots,0) = b_1$; ...; $f(0,0,\ldots,0,1) = b_n$, from which the values of any of the coefficients $c_1,\ldots,c_n$ can be found. So we continue; in general having considered all $f(x_1,\ldots,x_n)$, where q of the n variables $x_1,\ldots,x_n$ are equal to 1 (from which the values of all coefficients $c_{\nu_1\ldots\nu_q}$ are found), we proceed to consider any $f(x_1,\ldots,x_n)$ where q+1 of the variables are equal to 1. From such a relation which is linear in all $c_{\nu_1\ldots\nu_\rho}$ with $\rho \leq q+1$ and which contains only one such coefficient with $\rho = q+1$, this coefficient $c_{\nu_1\ldots\nu_{q+1}}$ is found. This proves the theorem.

We remark that the proof of the theorem in fact consisted of nothing but showing that the determinant $|d_{rs}|$ of the coefficients d in our system of 2^n linear equations is different from zero. The unknown $c_{\nu_1\ldots\nu_p}$ were ordered in such a way that $d_{rs} = 1$ for $r = s$ and $d_{rs} = 0$ for $r > s$, hence $|d_{rs}| = 1 \neq 0$.

The fundamental theorem may be generalised as follows. Consider functions $f(x_1,\ldots,x_n)$ of n variables which together with the function itself, may only assume the values $0,1,\ldots,p-1$ (here p denotes a prime number). Every such function (which assumes for any given set $(x_1,\ldots,x_n)$ an admissible prescribed value) may be written in the form

$$f(x_1,\ldots,x_n) = \sum\!\!\!\!\!\!- c_{\nu_1\ldots\nu_n}\, x_1^{\nu_1} \ldots x_n^{\nu_n}$$

where the sum is extended over all sets $(\nu_1,\ldots,\nu_n)$ with $0 \leqq \nu_\varrho \leqq p-1$ $(\varrho = 1,\ldots,n)$.

The proof runs in a similar way; one can show that the coefficients c can be found from a set of p^n linear equations. The coefficients c and the equations can be ordered in such a way that the determinant $D_p^{(n)}$ of the system is the compound determinant of order p^n in which the "element" in the r_1^{th} row s_1^{th} column is equal to $r^s\, D_p^{(n-1)}$ with

$r = \left[\frac{r_1}{p^{n-1}}\right]$; $s = \left[\frac{s_1}{p^{n-1}}\right]$. Herefrom one finds using the theorem of van der Monde:

$$D_p^{(n)} = ((p-1)!!)^{p^{n-1}}\, (D_p^{(n-1)})^p$$

hence by $D_p^{(1)} = (p-1)!!$ (van der Monde)

$$D_p^{(n)} = ((p-1)!!)^{np^{n-1}}.$$

Here a!! denotes the product $1!2!\ldots a!$.
Since $D_p^{(n)} \not\equiv 0 \pmod p$ (for p is prime) the generalisation of the fundamental theorem is proved. One has $D_2^{(n)} = 1$ (confer the above result).

§ 4. Operators.

We now consider systems of n functions $f_\nu(x_1,\ldots,x_n)$ $(\nu = 1,\ldots,n)$ of n variables, where again each of the functions as well as each of the variables may be equal only to 0 or 1. From the fundamental theorem in the preceding chapter we infer the fundamental theorem on systems of functions, which says:

There exists always at least one system $(f_1,\ldots,f_n)$ of n functions of n variables $x_1,\ldots,x_n$, which takes arbitrary prescribed values $(y_1,\ldots,y_n)$ for any set $(x_1,\ldots,x_n)$. All these functions f_ν are of the type (1) from § 3.

For by the fundamental theorem on functions a function f_ν exists which assumes an arbitrary prescribed value y_ν for every set $(x_1,\ldots,x_n)$ $(\nu = 1,\ldots,n)$, which proves the theorem.

Let us denote the equations $y_\nu = f_\nu(x_1,\ldots,x_n)$ $(\nu = 1,\ldots,n)$ shortly by $y = Fx$, where the operator F is determined by the functions $f_1,\ldots,f_n$. Since for every ν there exists only a finite number (namely 2^{2^n}) of functions $f_\nu(x_1,\ldots,x_n)$, the total number of different operators F is finite and equal to $2^{n2^n} = (2^n)^{2^n}$.

If another set of functions $g_\nu(y_1,\ldots,y_n)$ are given, such that the operator G which is defined by the g_ν belongs to the class of operators under consideration, one has $z_\nu = g_\nu(y_1,\ldots,y_n)$, hence $z_\nu = g_\nu(y_1(x_1,\ldots,x_n),\ldots,y_n(x_1,\ldots,x_n)) = h_\nu(x_1,\ldots,x_n)$, where the functions h_ν again define an operator H of the considered type. We write

$$z = Gy = GFx = Hx; \quad H = GF.$$

Due to the associative law for the crdinary operations one obtains for every three operators F_1, F_2 and F_3

$$(F_1F_2)F_3 = F_1(F_2F_3).$$

Further there exists an operator E with $Ex = x$. For take $e_\nu(x_1,\ldots,x_n) = x_\nu$ $(\nu = 1,\ldots,n)$, then $E = (e_1,\ldots,e_n)$. The property $E^r = E$ for alle positive integers r is obvious. One has for every operator F the property $FE = EF = F$. Since our class of operators is finite the sequence

$$F, F^2, F^3,\ldots$$

cannot contain for every F an infinite number of different operators. Let r be the smallest integer with $F^r = F^s$ $(r > s)$. Call $r-s = v$. Then $F^{s+a} = F^{s+a+nv}$ for all integers a and $n \geqq 0$. If $r_1 > r$, then putting $r_1 - s = qv + r_2$ $(0 \leqq r_2 < v)$, one has

$$F^{r_1} = F^{qv+s+r_2} = F^{r_2}F^{(q-1)v}F^r = F^{r_2}F^{(q-1)v}F^s = F^{r_2}F^{(q-2)v}F^r =$$

$$= F^{r_2}F^{(q-2)v}F^s = \ldots = F^{r_2}F^vF^s = F^{r_2}F^r = F^{r_2}F^s = F^{r_3},$$

where $r_3 = r_2 + s < v + s = r$. Hence for all integer $r_1 > r$ an integer $r_3 < r$ can be found such that $F^{r_1} = F^{r_3}$.

Herefrom follows that also s possesses a minimum property i.e. no $s_1 < s$ exists with $F^{s_1} = F^{r_1}$, for if such a s_1 would exist, one had because of the minimality of r certainly $r_1 > r$, hence an integer r_3 would exist with $r_3 < r$ and $F^{r_1} = F^{r_3}$, so that we would have $F^{s_1} = F^{r_3}$ with $r_3 < r$ contrary to hypothesis.

If an integer m exists with $F^{m_1} = E$ we can find in the sequence $F, F^2,\ldots,F^{m_1}$ the first operator m which is equal to E. Its exponent m will be called the period of F, which obviously must be a divisor of m_1. In this case the operator F possesses an inverse operator F^{-1} with $F^{-1}F = FF^{-1} = E$, for $F^{-1} = F^{m-1}$ satisfies. If conversely F possesses an inverse operator F^{-1} the operator F possesses an exponent for the above consisered numbers r and s with $r > s$ and $F^r = F^s$ exist in any way. Herefrom follows $(F^{-1})^sF^r = (F^{-1})^sF^s = E$, hence $F^v = E$, where $v = r - s$ is the period of F.

If $s = 0$ we call the element F cyclic; if $s > 0$ we call it periodic. Every element of our set of operators is periodic, not every element is cyclic.

That not all operators do possess an inverse, isshown by taking the operator defined by the functions $f_\nu(x_1,\ldots,x_n) = 0$ $(\nu = 1,\ldots,n)$, which we call the nulloperator Z. This operator possesses no inverse operator. Moreover one has for all operators F the relation $ZF = Z$, but $FZ = Z$ holds

only if in every $f_\nu(x_1,\ldots,x_n)$ the constant term is equal to zero.

One has obviously $Z^m = Z$ for all integer $m > 0$. The element Z is therefore not cyclic.

Theorem. If F possesses the property $Fx \neq Fx'$ for all two sets x and x' which are different, F possesses an inverse operator.

Proof. Consider all different sets $x = (x_1,\ldots,x_n)$ and the corresponding values $y = Fx = (y_1,\ldots,y_n)$ of Fx. Since all the sets y are different, by the fundamental theorem on operators we know the existence of an operator G which for a set y has the precribed corresponding value x. This operator G satisfies $y = Fx = FGy$, hence $FG = E$, and also $GFx = Gy = x$, hence $GF = E$.

In general if F possesses an inverse operator F^{-1} one has for all x, putting $y = Fx$, $F^{-1}Fx = F^{-1}y = x$ and $FF^{-1}y = Fx = y$ for all y.

Our operators work on a finite number N of elements and transform this set in a certain way in itself.

As soon as the N transformed elements are all different our operator belongs to the symmetric group $\mathfrak{S}_N$.

If, however, the N transformed elements may coincide our operators do not form a group since no inverse operator exists.

Consider a case where $M(<N)$ of the transformed elements are all different and the other N-M elements coincide in one or other way with these M elements. Let this transformation be performed by an operator A.

If the originals of the M elements are but a permutation of these elements the operator A be replaced by an operator A' which works on the M elements in the same way as A, while the transforms of the other N-M elements are arbitrary but all different and also different from the M elements under consideration. The operator A' then belongs to the symmetric group $\mathfrak{S}_M$ and in many cases one can consider A' instead of A.

In general, given any operator A we first investigate which elements $x^{(1)},\ldots,x^{(M)}$ are transformed into M different elements $x'^{(1)},\ldots,x'^{(M)}$, the set of which does not necessary coincide with the set $(x^{(1)},\ldots,x^{(M)})$. Always A can be replaced by an operator A' with the property that $x^{(M+1)},\ldots,x^{(N)}$ are transformed such that $x'^{(1)},\ldots,x'^{(N)}$ are a permutation of $x^{(1)},\ldots,x^{(N)}$, while $x^{(1)},\ldots,x^{(M)}$ retain their transforms.

As soon as the sets $(x^{(1)},\ldots,x^{(N)})$ and $(x^{(1)},\ldots,x'^{(M)}$ have the property that 10 elements of the first set are transformed by A into the same 10 elements in an arbitrary permutation, then A is usefull to be an addition or multiplication operator, or: As soon as A works on 10 elements in the same way as an operator of $\mathfrak{S}_{10}$, then A is a usefull operator.

We have reason to divide the operators A in usefull and not usefull operators. Every usefull operator corresponds with a set of $M(\geq 10)$ elements which are permutated by A. Once a usefull operator is chosen, this set is fixed. The product of two usefull operators A_1 and A_2 is not necessarily usefull, for the corresponding sets of M_1 and M_2 elements (which are permutated by A_1 resp. A_2), need not contain an intersection of $M(\geq 10)$

elements. If any set S of $M(\geqq 10)$ elements is permutated by an operator A, we call A a S-usefull operator. It is obvious that the product of two S-usefull operators is an S-usefull operator and further that all S-usefull operators A can be replaced by S-usefull operators A' (in the same way as above A was replaced by A'), which form a group.

We finally are only interested in the way in which the set S is transformed by the S-usefull operators.

For instance if $n = 4$, so that every integer 0,1,...,9 possesses 4 coordinates, which are 0 or 1, then $N = 16$ and we are only interested in S-usefull operators A which permutate at least the 10 elements 0,1,...,9, while the other 6 quadruples are transformed in a way we are not interested in, but which may be changed so as to make A equal to an operator A' of $\mathfrak{S}_{16}$.

Theorem. In our system of operators there exist cyclic operators with every period $m \leqq N$.

For let m be arbitrary $\leqq N$. Take m arbitrary different sets $(x_1,\ldots,x_n)$, which we denote by $x^{(1)}, x^{(2)},\ldots,x^{(m)}$.

By the fundamental theorem on operators an operator exist which transforms $x^{(1)}$ into $x^{(2)}$, $x^{(2)}$ into $x^{(3)},\ldots,$ $x^{(m-1)}$ into $x^{(m)}$ and finally $x^{(m)}$ into $x^{(1)}$ and which leaves all other N-m sets $(x_1,\ldots,x_n)$ invariant. Obvious this operator has the period m.

The number of different cyclic operators with period m found in this way from $x^{(1)}, x^{(2)},\ldots,x^{(m)}$ is equal to $\varphi(m)$, hence the total number of cyclic operators with period m by choosing in any way m from the N possible sets $(x_1,\ldots,x_n)$ is therefore equal to $\sum_{m=1}^{N} \varphi(m)\binom{N}{m}$. Moreover for any $d \mid m$ one finds $\varphi(d)\binom{N}{m}$ operators with period d hence in total we find already

$$\sum_{m=1}^{N}\sum_{d\mid m} \varphi(d)\binom{N}{m} = \sum_{m=1}^{N} m\binom{N}{m} = N\,2^{N-1}$$

different cyclic operators.

Also a cyclic operator can be found which transforms a set $x^{(1)}$ into $x^{(2)}$, $x^{(2)}$ into $x^{(3)}\ldots$, $x^{(m_1-1)}$ into $x^{(m_1)}$, $x^{(m_1)}$ into $x^{(1)}$; further $x^{(m_1+1)}$ into $x^{(m_1+2)},\ldots,x^{(m_1+m_2)}$ into $x^{(m_1+1)},\ldots,x^{(m_1+\ldots+m_{k-1}+1)}$ into $x^{(m_1+\ldots+m_{k-1}+2)},\ldots,x^{(m_1+\ldots+m_k)}$ into $x^{(m_1+\ldots+m_{k-1}+1)}$. Here $\sum_{k=1}^{k} m_k = N$; taking $m_2 = m_3 = \ldots = m_k = 1$ we obtain the original transformation for $m_1 = m$.

There exist

$$\frac{N!}{m!m_2!\ldots m_k!}$$

different such partitions of the number N which furnish us with

$$\sum_{\Sigma m_k = N} \varphi(M)\,\frac{N!}{m_1!\ldots m_k!}$$

different operators of period M, where M is the least common multiple of $m_1,\ldots,m_k$.

§5. Weights.

Once the numbers $x = 0,1,\ldots,9$ are coded we remark that the coordinates $(x_1,\ldots,x_n)$ of their code satisfy a relation

(1) $$x = g(x_1,\ldots,x_n) = g + g_1x_1 + \ldots + g_nx_n + g_{12}x_1x_2 + \ldots + g_{12\ldots}x_1x_2x_3 + \ldots$$

where the righthand side contains at most 10 terms, for this righthand side has to be equal to x for the set $(x_1,\ldots,x_n)$ i.e. has to assume a prescribed value for any of the given occuring systems $(x_1,\ldots,x_n)$, from which fact the fundamental theorem on functions learns us the existence of 10 coefficients g so as to satisfy (1). The coefficients g are called the weights of the representation of x by its coordinates $(x_1,\ldots,x_n)$.

If the coordinates $(x_1,\ldots,x_4)$ of x correspond with the number x written in the binary system as $x_1x_2x_3x_4$ one obviously has

$$x = 8x_1 + 4x_2 + 2x_3 + x_4.$$

For a number $x \geq 10$ where each of the decimal places itself is written in the binary notation, say $x = x_1x_2x_3x_4,\ x_5x_6x_7x_8$ were $x < 100$, one has

$$x = 80x_1 + 40x_2 + 20x_3 + 10x_4 + 8x_5 + 4x_6 + 2x_7 + x_8.$$

If such a number were entirely written in the binary system, only 7 coordinates would be sufficient and one would have

$$x = 64x_1 + 32x_2 + 16x_3 + 8x_4 + 4x_5 + 2x_6 + x_7.$$

The coding of every decimal digit separately is inefficient in so much one is concerned to reduce the number of necessary coordinates, which is due to the fact already mentioned in § 1, that 10 is much nearer to the highest power of 2 which is less than 10 than to the next power of 2.

The difference between the necessary binary coordinates and the number of coordinates used in the decimal-binary-coding increases with the number x. There are, however, advantages which justify the use of the decimal-binary coding.

§6. Addition of coded numbers.

We consider again the sum operator A which gives us the coordinates of the sum of two numbers x and y from the coordinates of these numbers

$$\begin{cases} s_\nu = s_\nu(x_1,\ldots,x_n;\ y_1,\ldots,y_n) \\ t_\nu = t_\nu(x_1,\ldots,x_n;\ y_1,\ldots,y_n) \end{cases} \qquad (\nu = 1,\ldots,n).$$

Let us first consider the functions s_ν. Calling the operators

$(s_1,\ldots,s_n) = S$ one has

$$x + y = S(x,y).$$

Once an arbitrary way of coding of the integers $0,1,\ldots,9$ is given the fundamental theorem learns us the existence of an operator S which for every of the 100 possibilities $(x_1,\ldots,x_n; y_1,\ldots,y_n)$ gives us the n coordinates $s_1,\ldots,s_n$ of $s = x + y$.

Let us for a moment fix $y = 1$. Then one obtains the addition of 1, which we denote by A_1. One has $x + 1 = A_1x$. Moreover, in general we shall write $x + y = A_yx$. We have $A_y = A_1^y$.

The operators $A_1^o = E, A_1, \ldots, A_1^s$ form a group with

$$A_1^r A_1^s = A_1^t, \text{ where } t \equiv r + s \pmod{10},$$

which is isomorphic with the addition group of the integers (mod 10). This group is determined by the choice of A_1, but may also be determined by any other of the $\varphi(10)$ numbers A_λ with $(\lambda,10)=1$, for instance by A_3.

We further remark that the transformation $x' = f(x)$ gives

$$A'_yx = x + y' = x + f(y) \cdot = A_{f(y)}x$$

and putting $B_y = A'_y$ one gets

$$B_yx = A_{f(y)}x.$$

Hence the transformation $x' = f(x)$ induces a transformation of operator $B_y = A_{f(y)}$, where $B_y = A'_y$.

As soon as the operator A_1 with $A_1^{10} = E$ is given and a codation of one of the integers $0,1,\ldots,9$ is assumed, the codation of all other nine integers follows by applying A_1 sufficiently often to the given integer.

We see that the codation of the ten integers determines the operator A_1 and inversely the codation of one integer determines, if A_1 is given, the codation of the others.

The same holds if in this argument A_1 is replaced by A_3, A_7 or A_9.

As soon as either A_1 and the coding of one integer or the coding of all ten integers $0,1,\ldots,9$ is given, the general addition formulae are fixed.

Conversely, if the general addition formulae are fixed, the coding of 0 follows from the equation $x = x + x$. The general addition formulae may not be given arbitrarily for one has for instance $S(\ldots S(S(S(x,y)y),y),y)\ldots),y) = x$ for all x and y where 10 operators S are applied.

Once the integers $0,1,\ldots,9$ are coded, the operator $T(x,y)$ determined by the n functions $t_1(x,y),\ldots,t_n(x,y)$ is fixed. Obviously $T(x,y)$ assumes only two sets of values, namely those corresponding to the integer 0 and to the integer 1.

Any operator T which assumes for nine given sets $(x_1,\ldots,x_n)$ a same value $(z_1,\ldots,z_n)$ occuring among these nine sets and for the tenth set

$\neq (z_1,\ldots,z_n)$ occuring among the nine given sets, may be taken as $T(x,1)$.

As soon as $T(x,1)$ is given, the coding of 0,1 and 9 is fixed, for one has $(z_1,\ldots,z_n) = 0$; $(y_1,\ldots,y_n) = 9$; $(u_1,\ldots,u_n) = 1$. Hence by $T(x,1)$ and the coding of $2,3,\ldots,8$ the coding of all integers $0,1,\ldots,9$ is fixed.

The degree of the operator S in $x_1,\ldots,x_n$, $y_1,\ldots,y_n$ depends on the degree k of the operator A_1. Putting $y = 1$ the operator S becomes equal to A_1, hence S is of a degree $\geqq k$ in the coordinates $x_1,\ldots,x_n$ and so is S in the coordinates $y_1,\ldots,y_n$.

§ 7. Multiplication of coded numbers.

Many properties of the preceeding paragraph do still hold, if one replaces the addition by multiplication.

The general multiplication operator M is the operator, which, given any two integers of the set $0,1,\ldots,9$, gives us two new integers corresponding to the decimal representation of their product. In § 2 we wrote for $0 \leqq x,y,p,q \leqq 9$

$$\left.\begin{aligned} p_\nu &= p_\nu\,(x_1,\ldots,x_n;\ y_1,\ldots,y_n) \\ q_\nu &= q_\nu\,(x_1,\ldots,x_n;\ y_1,\ldots,y_n) \end{aligned}\right\} \qquad (\nu = 1,\ldots,n),$$

where $xy = 10q + p$.

Taking y fixed we obtain multiplication formulae for $M_y x$, where M_y is the operator which transforms for a given y the number x into the number p, which is equal to $xy \pmod{10}$.

Evidently one has $M_1 = E$; $M_0 = Z$.

Besides each M has a period which divides $\varphi(10) = 4$, for for every y one has $y^{1+\varphi(10)} \equiv y \pmod{10}$ hence $M_y^{\varphi(10)+1} x = xy^{\varphi(10)+1} \equiv xy \pmod{10}$, hence $M_y^{\varphi(10)+1} = M_y$, hence for the smallest r with $M_y^r = E$ one must have $r \mid \varphi(10)$.

If $\left\{\begin{matrix} y \not\equiv 0 \pmod 2 \\ y \not\equiv 0 \pmod 5 \end{matrix}\right\}$, one has for instance $M_y^4 = M_6$.

As in § 6 one proves that given a codation of the integers $0,1,\ldots,9$ general multiplication formulae p and q can be found, which are entire and rational both in the coordinates x and y. About the degree of these formulae analoguous theorems exist to those proved in § 6.

§ 8. Choice of coding.

We now have to make our choice in which way the integers $0,1,\ldots,9$ shall be coded. We choose such a coding that the machines are as simple as possible. In this connection it be remarked that the apparatus necessary to compute the sum mod 2 of two integers (each of which is equal to 0 or 1) is much more complicated than the one necessary for their product mod 2. This is due to the fact that the formula $1 + 1 \equiv 0 \pmod 2$ involves rather a complicated apparatus, while this is not the case with the formulae

$0 + 0 \equiv 0$; $0 + 1 \equiv 1 + 0 \equiv 1$, which are true also if the reduction mod 2 is not performed.

If we try to confine ourselves as much as possible to perform only such simpler operations (by which we mean operations which do not require the complicated apparatus to calculate $1 + 1 \equiv 0 (\mathrm{mod}\ 2)$), then for instance a sum $ab + (b+1)$, once all three numbers a, b and b+1 are coded, is also in a rather simple way to get. If only the numbers a and b are given this expression is more difficult to get, since the operation necessary to obtain b+1 from b is rather complicated. Once this last operation is admitted the sum a+b can be got from a and b by using twice this operation, since one has $a+b \equiv a(b+1) + b(a+1) \pmod 2$.

Further it be remarked that in general a product is the more complicated the more its number of factors increases, and that products of two factors are considerably more simple to get than those of 3 or more factors. On the other hand the formula $(x_h+1)(x_k+1)+1$ is as simply to be realised as the formula $x_h x_k$. Writing $\bar{x} = x+1$ one has $(x_h+1)(x_k+1)+1 = \overline{\bar{x}_h \bar{x}_k}$.

We now proceed to investigate a formula say for A_1, which from the practical point of view is as simple as possible.

Once the number n of coordinates is fixed by far the simplest operator A_1 would be the operator for which the coordinates of $x' \equiv x+1 \pmod{10}$ are merely a permutation of those of x. Since such an operator has a period which divides n! and since A_1 possesses the period 10, one must obviously have $n \geqq 5$, although as we remarked a codation with n=4 would theoretically apart from the permutation condition already be sufficient. The condition $10 \mid n!$, however, is necessary but not sufficient, since the symmetric group $\mathfrak{S}_n$ contains only elements of which the period is a least common multiple of any set $n_1,\ldots,n_k$ with $n_1+\ldots+n_k = n$. Herefrom follows that n cannot be equal to 5, neither to 6, so that the first possibility for a representation of all integers $0,1,\ldots,9$ by n coordinates, such that addition formulae are but permutations of coordinates occurs for n=7. This case, for which the formulae will be given in the next paragraph, has a simple addition but by no means a simple multiplication theorem. So there is sufficient reason to drop the condition that our operators are but permutators.

Since every operator consists of a set of polynomials in the coordinates instead of allowing but one term to occur in those polynomials we now allow them to possess more terms.

In view of the difficulty of performing the addition 1+1 and multiplications with more than two factors our polynomials may contain but one linear term and only such a number of quadratic terms that one is sure that not two of them are at the same time equal to 1. In §11 we shall investigate systematically all possibilities for n=4, which satisfy these conditions.

§ 9. A way of coding for n=7.

In the simplest case where the symmetrical group possesses elements of order 10, i.e. the case n=7, we only have to take for A_1 any operator of order 10, and make an arbitrary choice for the coordinates of one of the integers 0,1,...,9, say those of zero. We take for instance 0= =(0 0 0 0 1 0 1); let A_1 be given by the formulae

$$\begin{cases} x_1' = f_1(x) = x_5 \\ x_2' = x_1 \\ x_3' = x_2 \\ x_4' = x_3 \\ x_5' = x_4 \\ x_6' = x_7 \\ x_7' = x_6 \end{cases}$$

Then one gets

$$\begin{cases} 0 = (0\ 0\ 0\ 0\ 1\ 0\ 1) \\ 1 = (1\ 0\ 0\ 0\ 0\ 1\ 0) \\ 2 = (0\ 1\ 0\ 0\ 0\ 0\ 1) \\ 3 = (0\ 0\ 1\ 0\ 0\ 1\ 0) \\ 4 = (0\ 0\ 0\ 1\ 0\ 0\ 1) \\ 5 = (0\ 0\ 0\ 0\ 1\ 1\ 0) \\ 6 = (1\ 0\ 0\ 0\ 0\ 0\ 1) \\ 7 = (0\ 1\ 0\ 0\ 0\ 1\ 0) \\ 8 = (0\ 0\ 1\ 0\ 0\ 0\ 1) \\ 9 = (0\ 0\ 0\ 1\ 0\ 1\ 0). \end{cases}$$

The general addition formulae which give us the coordinates of the sum s of two integers x and y (all mod 10) are of the form

$$s_\nu = \sum_{i,j} c_{\nu ij} x_i y_j$$

One gets

$$\begin{cases} s_1 = x_1 y_5 + x_2 y_4 + x_3 y_3 + x_4 y_2 + x_5 y_1 \\ s_2 = x_1 y_1 + x_2 y_5 + x_3 y_4 + x_4 y_3 + x_5 y_2 \\ s_3 = x_1 y_2 + x_2 y_1 + x_3 y_5 + x_4 y_4 + x_5 y_3 \\ s_4 = x_1 y_3 + x_2 y_2 + x_3 y_1 + x_4 y_5 + x_5 y_4 \\ s_5 = x_1 y_4 + x_2 y_3 + x_3 y_2 + x_4 y_1 + x_5 y_5 \\ s_6 = x_6 y_7 + x_7 y_6 \\ s_7 = x_6 y_6 + x_7 y_7. \end{cases}$$

Since only one of the first five coordinates differs from zero, all sums for $s_1,\ldots,s_5$ are simple and this is also true for s_6 and s_7 since either x_6 or x_7 is equal to 1.

Our general product formulae p = xy now become

$$p_1 = x_1 y_1 + x_2 y_3 + x_3 y_2 + x_4 y_4$$

$$p_2 = x_1 y_2 + x_2 y_1 + x_3 y_4 + x_4 y_3$$

$$p_3 = x_1 y_3 + x_2 y_4 + x_3 y_1 + x_4 y_2$$

$$p_4 = x_1 y_4 + x_2 y_2 + x_3 y_3 + x_4 y_1$$

$$p_5 = \overline{\bar{x}_5\ \bar{y}_5}$$

$$p_6 = \overline{\bar{x}_6\ \bar{y}_6}$$

$$p_7 = \overline{\bar{x}_7\ \bar{y}_7}\ .$$

In this case the addition and multiplication formulae for the carry t_ν resp. q_ν , are

$t_2 = t_3 = t_4 = 0$

$$t_1 = t_6 = x_1x_6y_4y_6 + x_2x_7y_3y_7 + x_2x_7y_4y_6 + x_3x_6y_2y_6 + x_3x_6y_3y_7 + x_3x_6y_4y_6 +$$
$$+ x_4x_7y_1y_7 + x_4x_7y_2y_6 + x_4x_7y_3y_7 + x_4x_7y_4y_6 + x_5x_6y_5y_6 + x_5x_6y_1y_7 +$$
$$+ x_5x_6y_2y_6 + x_5x_6y_3y_7 + x_5x_6y_4y_6 + x_1x_7y_4y_7 + x_1x_7y_5y_6 + x_1x_7y_1y_7 +$$
$$+ x_1x_7y_2y_6 + x_1x_7y_3y_7 + x_1x_7y_4y_6 + x_2x_6y_3y_6 + x_2x_6y_4y_7 + x_2x_6y_5y_6 +$$
$$+ x_2x_6y_1y_7 + x_2x_6y_2y_6 + x_2x_6y_3y_7 + x_2x_6y_4y_6 + x_3x_7y_2y_7 + x_3x_7y_3y_6 +$$
$$+ x_3x_7y_4y_7 + x_3x_7y_5y_6 + x_3x_7y_1y_7 + x_3x_7y_2y_6 + x_3x_7y_3y_7 + x_3x_7y_4y_6 +$$
$$+ x_4x_6y_1y_6 + x_4x_6y_2y_7 + x_4x_6y_3y_6 + x_4x_6y_4y_7 + x_4x_6y_5y_6 + x_4x_6y_1y_7 +$$
$$+ x_4x_6y_2y_6 + x_4x_6y_3y_7 + x_4x_6y_4y_6\ .$$

$$t_5 = t_7 = x_5x_7y_5y_7 + x_5x_7y_1y_6 + x_5x_7y_2y_7 + x_5x_7y_3y_6 + x_5x_7y_4y_7 + x_5x_7y_5y_6 +$$
$$+ x_5x_7y_1y_7 + x_5x_7y_2y_6 + x_5x_7y_3y_7 + x_5x_7y_4y_6 + x_1x_6y_5y_7 + x_1x_6y_1y_6 +$$
$$+ x_1x_6y_2y_7 + x_1x_6y_3y_6 + x_1x_6y_4y_7 + x_1x_6y_5y_6 + x_1x_6y_1y_7 + x_1x_6y_2y_6 +$$
$$+ x_1x_6y_3y_5 + x_2x_7y_4y_7 + x_2x_7y_5y_6 + x_2x_7y_1y_7 + x_2x_7y_2y_6 + x_2x_7y_5y_7 +$$
$$+ x_2x_7y_1y_6 + x_2x_7y_2y_7 + x_2x_7y_3y_6 + x_3x_6y_5y_7 + x_3x_6y_1y_6 + x_3x_6y_2y_7 +$$
$$+ x_3x_6y_3y_6 + x_3x_6y_4y_7 + x_3x_6y_5y_6 + x_3x_6y_1y_7 + x_4x_7y_5y_7 + x_4x_7y_1y_6 +$$
$$+ x_4x_7y_2y_7 + x_4x_7y_3y_6 + x_4x_7y_4y_7 + x_4x_7y_5y_6 + x_5x_6y_5y_7 + x_5x_6y_1y_6 +$$

$$+ x_5x_6y_2y_7 + x_5x_6y_3y_6 + x_5x_6y_4y_7 + x_1x_7y_5y_7 + x_1x_7y_1y_6 + x_1x_7y_2y_7 +$$
$$+ x_1x_7y_3y_6 + x_2x_6y_5y_7 + x_2x_6y_1y_6 + x_2x_6y_2y_7 + x_3x_7y_5y_7 + x_3x_7y_1y_6 +$$
$$+ x_4x_6y_5y_7,$$

$$q_1 = x_2x_7y_5y_6 + x_2x_7y_1y_7 + x_2x_7y_2y_6 + x_2x_7y_3y_7 + x_2x_7y_4y_6 + x_3x_6y_4y_7 + x_3x_6y_5y_6 +$$
$$+ x_3x_6y_1y_7 + x_4x_7y_4y_7 + x_5x_6y_2y_7 + x_1x_7y_2y_7 + x_2x_6y_2y_7 + x_3x_7y_2y_7 + x_4x_6y_2y_7 +$$
$$+ x_4x_7y_3y_6 + x_5x_6y_3y_6 + x_1x_7y_3y_6 + x_2x_6y_4y_6 + x_4x_6y_2y_6 + x_3x_7y_3y_7 .$$

$$q_2 = x_3x_6y_2y_6 + x_3x_6y_3y_7 + x_3x_6y_4y_6 + x_4x_7y_5y_6 + x_4x_7y_1y_7 + x_4x_7y_2y_6 + x_6x_7y_6y_7 +$$
$$+ x_2x_6y_3y_6 + x_3x_7y_3y_6 + x_4x_6y_3y_6 + x_5x_6y_4y_7 + x_1x_7y_4y_7 + x_2x_6y_4y_7 + x_3x_7y_4y_6 +$$
$$+ x_4x_6y_3y_7 ,$$

$$q_3 = x_4x_7y_3y_7 + x_3x_7y_4y_7 + x_5x_6y_2y_6 + x_2x_6y_5y_6 + x_1x_7y_1y_7 + x_3x_7y_3y_7$$

$$q_4 = x_5x_6y_3y_7 + x_3x_7y_5y_6 + x_1x_7y_2y_6 + x_2x_6y_1y_7 + x_6x_7y_4y_6 + x_4x_6y_6y_7 + x_2x_6y_2y_6$$

$$q_5 = x_1x_6y_5y_7 + x_1x_6y_5y_7 + x_2x_7y_2y_7 + x_2x_7y_3y_6 + x_2x_7y_4y_7 + x_3x_6y_3y_6 + x_2x_6y_3y_7 +$$
$$+ x_3x_6y_2y_7 + x_4x_7y_2y_7 + x_1x_7y_4y_6 + x_4x_6y_1y_7 + x_3x_7y_2y_6 .$$

$$q_6 = x_1x_6y_5y_7 + x_4x_6y_4y_6 + x_2x_7y_2y_7 + x_2x_7y_3y_6 + x_2x_7y_4y_7 + x_3x_6y_3y_6 + x_3x_6y_2y_6 +$$
$$+ x_3x_6y_3y_7 + x_5x_7y_1y_6 + x_3x_7y_3y_7 + x_2x_6y_2y_6 + x_3x_6y_2y_7 + x_4x_7y_2y_7 + x_5x_6y_5y_6 +$$
$$+ x_2x_6y_3y_6 + x_3x_7y_3y_6 + x_2x_6y_4y_6 + x_3x_6y_4y_6 + x_4x_7y_5y_6 + x_4x_7y_1y_7 + x_4x_7y_2y_6 +$$
$$+ x_5x_6y_3y_7 + x_5x_6y_4y_6 + x_1x_7y_2y_6 + x_1x_7y_3y_7 + x_4x_6y_2y_6 + x_4x_6y_3y_6 + x_5x_6y_4y_7 +$$
$$+ x_1x_7y_4y_7 + x_2x_6y_4y_7 + x_3x_7y_5y_6 + x_4x_6y_5y_6 + x_2x_6y_1y_7 + x_3x_7y_1y_7 .$$

$$q_7 = x_2x_7y_5y_6 + x_2x_7y_1y_7 + x_2x_7y_2y_6 + x_2x_7y_3y_7 + x_2x_7y_4y_6 + x_3x_6y_4y_7 + x_3x_6y_5y_6 +$$
$$+ x_5x_6y_2y_7 + x_1x_7y_2y_7 + x_2x_6y_2y_7 + x_3x_7y_2y_7 + x_4x_6y_2y_7 + x_4x_7y_3y_6 + x_5x_6y_3y_6 +$$
$$+ x_3x_6y_1y_7 + x_4x_7y_4y_7 + x_4x_7y_3y_7 + x_4x_7y_4y_6 + x_5x_6y_1y_7 + x_5x_6y_2y_6 + x_1x_7y_4y_6 +$$
$$+ x_1x_7y_3y_6 + x_1x_7y_1y_7 + x_3x_7y_4y_7 + x_4x_6y_4y_7 + x_1x_7y_5y_6 + x_2x_6y_5y_6 + x_4x_6y_1y_7 +$$
$$+ x_2x_6y_3y_7 + x_3x_7y_4y_6 + x_3x_7y_2y_6 + x_4x_6y_3y_7 .$$

§ 10. A coding for n=5.

The 7 coordinates as they were introduced in the preceding paragraph are not independent. One has $x_1+\ldots+x_5=1$; $x_6+x_7=1$. Hence all formulae

may be simplified by expressing x_5 and x_7 in the other 5 coordinates. If then x_6 is called x_5, we obtain

$$\begin{cases} 0 = (0\ 0\ 0\ 0\ 0) \\ 1 = (1\ 0\ 0\ 0\ 1) \\ 2 = (0\ 1\ 0\ 0\ 0) \\ 3 = (0\ 0\ 1\ 0\ 1) \\ 4 = (0\ 0\ 0\ 1\ 0) \\ 5 = (0\ 0\ 0\ 0\ 1) \\ 6 = (1\ 0\ 0\ 1\ 0) \\ 7 = (0\ 1\ 0\ 0\ 1) \\ 8 = (0\ 0\ 1\ 1\ 0) \\ 9 = (0\ 0\ 0\ 1\ 1) \end{cases}$$

and the general sumformulae for s = x+y become

$$\begin{cases} s_1 = x_1y + x_2y_4 + x_3y_3 + x_4y_2 + x\,y_1 \\ s_2 = x_1y_1 + x_2y + x_3y_4 + x_4y_3 + x\,y_2 \\ s_3 = x_1y_2 + x_2y_1 + x_3y + x_4y_4 + x\,y_3 \\ s_4 = x_1y_3 + x_2y_2 + x_3y_1 + x_4y + x\,y_4 \\ s_5 = x_5 + y_5 \end{cases}$$

where $x = \overline{x_1 + x_2 + x_3 + x_4}$; $y = \overline{y_1 + y_2 + y_3 + y_4}$.

Our product formulae become:

$$p_1 = x_1y_1 + x_2y_3 + x_3y_2 + x_4y_4$$

$$p_2 = x_1y_2 + x_2y_1 + x_3y_4 + x_4y_3$$

$$p_3 = x_1y_3 + x_2y_4 + x_3y_1 + x_4y_2$$

$$p_4 = x_1y_4 + x_2y_2 + x_3y_3 + x_4y_1$$

$$p_5 = x_5\,y_5$$

The carries are found from

$q_1 =$

	x_1	x_2	x_3	x_4	1
y_1	0	$\bar{x}_5$	x_5	0	0
y_2	$\bar{y}_5$	0	$\bar{y}_5+x_5y_5$	x_5y_5	$\overline{x_5\bar{y}_5}$
y_3	y_5	$\bar{x}_5+x_5y_5$	$\bar{x}_5\bar{y}_5$	y_5	x_5y_5
y_4	0	x_5y_5	x_5	$\bar{x}_5\bar{y}_5$	0
1	0	$\overline{x_5y_5}$	x_5y_5	0	0

where the right hand side denotes the sum $\sum_{i,j=1} a_{ij}x_iy_j$ (with $x_5=y_5=1$) in which the coefficients a_{ij} are found from the scheme, for instance $a_{13}=y_5$.

$q_2 =$

	x_1	x_2	x_3	x_4	1
y_1	$x_5\bar{y}_5$	x_5	$x_5\bar{y}_5$	$x_5\bar{y}_5$	$\overline{x_5\bar{y}_5}$
y_2	y_5	0	x_5y_5	x_5y_5	x_5y_5
y_3	$\bar{x}_5y_5$	x_5y_5	0	$\overline{\bar{x}_5\bar{y}_5}$	0
y_4	$\bar{x}_5y_5$	x_5y_5	$\bar{x}_5\bar{y}_5$	$\overline{\bar{x}_5\bar{y}_5}$	0
1	$\bar{x}_5y_5$	x_5y_5	0	0	0

$q_3 =$

	x_1	x_2	x_3	x_4	1
y_1	0	$x_5\bar{y}_5$	$\bar{x}_5$	x_5y_5	0
y_2	$\bar{x}_5y_5$	x_5y_5	$\bar{x}_5y_5$	x_5y_5	0
y_3	$\bar{y}_5$	$x_5\bar{y}_5$	x_5+y_5	x_5	$\overline{x_5\bar{y}_5}$
y_4	x_5y_5	x_5y_5	y_5	0	x_5y_5
1	0	0	$\overline{\bar{x}_5y_5}$	x_5y_5	0

$q_4 =$

	x_1	x_2	x_3	x_4	1
y_1	x_5y_5	x_5y_5	x_5y_5	$\bar{x}_5+x_5y_5$	x_5y_5
y_2	x_5y_5	x_5y_5	0	x_5y_5	x_5y_5
y_3	x_5y_5	0	$\overline{\bar{x}_5\bar{y}_5}$	x_5+y_5	x_5y_5
y_4	$\bar{y}_5+x_5y_5$	x_5y_5	x_5+y_5	$\overline{\bar{x}_5\bar{y}_5}$	x_5
1	x_5y_5	x_5y_5	x_5y_5	y_5	x_5y_5

$q_5 =$

	x_1	x_2	x_3	x_4	1
y_1	$\overline{x_5y_5}$	1	x_5y_5	0	$\overline{x_5\bar{y}_5}$
y_2	1	0	$\overline{x_5y_5}$	x_5y_5	x_5
y_3	x_5y_5	$\overline{x_5y_5}$	0	1	x_5y_5
y_4	0	x_5y_5	1	$\overline{x_5y_5}$	0
1	$\overline{\bar{x}_5y_5}$	y_5	x_5y_5	0	0

Finally one obtains for the addition carry

$t_2 = t_3 = t_4 = 0$

$t_1 = t_5 =$

	x_1	x_2	x_3	x_4	1
y_1	1	0	1	$\bar{x}_5+y_5$	x_5
y_2	0	x_5+y_5	$\bar{x}_5+y_5$	x_5+y_5	0
y_3	1	$x_5+\bar{y}_5$	$x_5+\bar{y}_5$	$x_5+\bar{y}_5$	x_5
y_4	$x_5+\bar{y}_5$	x_5+y_5	$\bar{x}_5+y_5$	x_5+y_5	0
1	y_5	0	y_5	0	0

§ 11. The coding with n=4.

We want to investigate the case n=4 a little closer. As we remarked before we confine ourselves to the case the transformations are at most of a degree 2 in the variables. First let us suppose the coding is taken in such a manner that at most two of the coordinates are different from zero. Then only the following formulae can occur for the polynomial operator A_1:

$$x_i \; ; \; x_i + x_j x_k \; ; \; x_i + x_j x_k + x_k x_l \; ; \; x_i + x_j x_k + x_k x_l + x_l x_j \; .$$
$$\bar{\bar{x}}_i \bar{\bar{x}}_j \; ; \; x_k x_l + \bar{\bar{x}}_i \bar{\bar{x}}_j \; ; \; \sum_{i,j} x_i x_j \; .$$

Let us first take the case where every integer $\geqq 0$ and $\leqq 9$ possesses exactly 1 or 2 coordinates which differ from zero. Then since there are 4 integers for which x_ν' (ν fixed) differs from zero, we consider the number of possibilities (x_1, x_2, x_3, x_4) for which anyone of the 7 above expressions can be equal to 1. Since we showed already that (x_1', x_2', x_3', x_4') cannot be a permutation of (x_1, x_2, x_3, x_4) one sees that for at least one ν one x_ν' is a non-linear expression in the x_μ of one of the six possible above mentioned forms. Let us consider these six forms successively.

1°. $x_i + x_j x_k$. This expression is equal to 1 either if $x_i = 1$; $x_j x_k = 0$ which gives 4 possibilities, one of $x_i = 0$; $x_j x_k = 1$, which is possible only in the case $x_j = x_k = 1$. Hence for 5 occurring integers x one has x'=1, contrary to the condition that this should happen for exactly four integers x.

2°. $x_i + x_j x_k + x_k x_l$. This expression is $\neq 0$ if:

$x_k = 0$; x_j, x_l arbitrary, which gives rise to 3 cases.

$x_i = 1$; $x_k = 1$; $x_j = x_l = 0$, which is 1 case.

$x_i = x_j$; $x_k = 0$; $x_k x_l \leqq 1$, which similarly involves the case $x_k = x_l = 1$.

Altogether our expression is $\neq 0$ in $6 \neq 4$ cases.

3°. $x_i + x_j x_k + x_k x_l + x_l x_j$.

The cases in which this expression is $\neq 0$ are

$x_i = 1$; x_j, x_k, x_l arbitrary 0 or 1 (but only one of them =1), which gives the 4 cases.

$x_k x_l = x_l x_j = x_i = 0$; $x_j x_k = 1$; hence $x_j = x_k = 1$; $x_i = x_l = 0$.
Similarly the cases; $x_k = x_l = 1$ and $x_l = x_j = 1$.
Altogether we get $7 (\neq 4)$ cases.

4°. $\bar{\bar{x}}_i \bar{\bar{x}}_j$. This expression is equal to 1 if either x_i or x_j or both are =0, which gives 3+3+1=7($\neq$ 4) cases.

5°. $\overline{x_i x_j} + x_k x_l$. This expression is equal to 1 if either $\overline{x_i x_j} = x_k x_l = 0$
hence $x_i = 1$; $x_j = 0$; $x_{k,l}$ arbitrary (3 cases)
$x_i = 0$; $x_j = 1$; $x_{k,l}$ arbitrary (3 cases)

or: $\bar{x}_i\bar{x}_j=1$; $x_kx_l=1$, hence $x_k=x_l=1$; $x_i=x_j=0$.
Altogether we get $8(\neq 4)$ cases.

6°. $x'_\nu = \sum_{i,j} x_ix_j$.

The sum may only in 4 cases be equal to one. Since at most one term can be equal to one, and since any such term =1 gives one possibility for x, our sum must contain exactly 4 terms; such a sum will be denoted by $\sum_4$.

So the only possibilities are:

$$x'_\nu = x_i;\quad x'_\nu = \sum_4 x_ix_j$$

and at least one of the 4 variables x'_ν must satisfy the second relation.

If exactly one of the variables x'_ν is quadratic in the x_μ, we have

6a
$$\begin{cases} x'_a = x_i \\ x'_b = x_j \\ x'_c = x_k \\ x'_d = \sum_4 x_r x_s. \end{cases}$$

We remark that either the term x_ix_j, or the term x_jx_k or the term x_ix_k occurs in $\sum_4$, hence there exists an integer x for which three of the coordinates of x' would be equal to one, which is impossible.

If two of the variables say x'_c and x'_d are non-linear, we have

6b
$$\begin{cases} x'_a = x_i \\ x'_b = x_j \\ x'_c = \sum_4 x_kx_l \\ x'_d = \sum_4 x_px_q\ . \end{cases}$$

For $x_i=x_j=1$ both x'_c and x'_d may but contain terms $\neq 1$, hence x_ix_j does not occur in $\sum_4$ and $\sum_4^*$, hence three terms of $\sum_4$ occur in $\sum_4^*$, while the fourth terms are different. A term x_jx_k may only make one of the two variables x'_c and $x'_d \neq 0$, hence any term x_jx_k does occur in only one of the sums $\sum_4$ and $\sum_4^*$. This holds for the 4 terms x_ix_k, x_ix_l; x_jx_k, x_jx_l, so $\sum_4$ and $\sum_4^*$ may contain together only 6+6-4-2 (namely x_ix_j)=6 terms, which is impossible.

6c A transformation

$$\begin{cases} x'_a = x_i \\ x'_b = \sum_4 x_kx_m \\ x'_c = \sum_4^* x_px_q \\ x'_d = \sum_4^{**} x_rx_s \end{cases}$$

gives for $x_i=1$; $x_j=1$ only at most one term in $\sum_4, \sum_4^*, \sum_4^{**}$ which may be

equal to 1, hence in the three sums which contain 12 terms, the 3 terms $x_i x_j$ are twice missing. Also any term $x_j x_k$ cannot occur in three of the sums, since then they all would be equal to 1. So from the 18 possible terms, 7 do not occur, which is impossible.

6d A transformation where each x' is transformed by a sum $\sum_4 x_k x_m$ does not occur, for any term $x_i x_j$ must miss in at least two of the sums, so they do contain together at most

$$4x6 - 2x6 = 12 \neq 16 \text{ terms.}$$

So not any transformation of the simple kind is possible for the operator A_1 in the case we code all integers with 4 coordinates of which either exactly 1 or exactly 2 differ from zero.