STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1954 - 010

Voordracht in de serie Actualiteiten

H.J.A. Duparc

24 april 1954

FROM RECURRING FRACTION TO RECURRING COMPUTING CIRCUIT

1954

Rapport ZW 1954-010.

Voordracht door H.J.A.Duparc in de serie

Actualiteiten op 24 April 1954.

FROM RECURRING FRACTION TO RECURRING COMPUTING CIRCUIT.

0. In this report several periodic processes are studied from a general point of view. One of these periodic processes - already familiar to us since the early days of the primary school - is the theory of recurring fractions ; another studied in a later stage of our mathematical life, is the theory of exponents of an integer modulo another integer. Both are aspects of the same kind of problems, viz. those on cyclic groups.

Here it is our intention to study also other processes which are necessarily periodic and can often be reduced to the above type; we mention the linear recurring sequences reduced modulo an integer and some other processes easily to be realised by simple computing circuits. Although the theory can be generalised further we treat only the here mentioned applications.

In all these processes besides the sequence $u_0, u_1, \ldots$ of integers the periodicity of which is investigated also another sequence $v_0, v_1, \ldots$ is introduced, the properties and period of which are closely connected to those of the original sequence.

1. Consider two sequences of integers

(u) $u_0, u_1, \ldots$

and

(v) $v_0, v_1, \ldots$,

satisfying the relations

(1) $U\, u_n = V\, v_n \qquad 0 \leqq u_n \leqq m-1 \qquad (n = 0, 1, \ldots)$,

where m is a fixed given positive integer and where

$$U = U(E) = \sum_{h=0}^{s} p_h E^h \quad \text{and} \quad V = V(E) = \sum_{k=0}^{t} q_k E^k$$

are given polynomials with integer coefficients in the operator E which transforms any u_n into u_{n+1} and any v_n into v_{n+1}.

The operators U and V are subject to the following conditions

I. $p_s = \pm 1$, $q_t = m$;

II. U(E) and V(E) are relatively prime ;

III. V(X) has no roots with absolute value $\geqq 1$.

The condition I assures the possibility of determining u_n (if $n \geqq s$)

and v_n (if $n \geqq t$) uniquely once the preceding elements of the sequences (u) and (v) are known.

2. Definition. A positive integer C is called a period of a sequence

(w) $\quad w_0, w_1, \ldots$

if an integer $N \geqq 0$ exists such that

$$w_{n+C} = w_n \qquad (n = N, N+1, \ldots).$$

The smallest positive period of the sequence is called the primitive period and will be denoted by C_w, the corresponding value of N by N_w. Obviously one has: If a sequence (w) has a period C then also its primitive period C_w exists and $C_w \mid C$. Conversely every multiple of the primitive period of a sequence is a period of the sequence.

The first relation (1) can be considered as a linear inhomogeneous difference equation for v. In this equation the term not depending on v is bounded; in fact its absolute value is $\leqq (m-1) \sum_{h=0}^{s} |p_h|$. Since by condition III the characteristic polynomial of the sequence has no roots with absolute value $\geqq 1$, every solution of this difference equation is bounded, i.e. the sequence (v) is bounded.

Since both sequences (u) and (v) appear to be bounded there is only a finite number of possible couples (u_n, v_n), hence the set of these couples, i.e. the considered process, is periodic. Then also the sequences (u) and (v) are periodic and after a little argument one finds that the primitive period $C = C_{uv}$ of the sequence of couples (u_n, v_n) is equal to the least common multiple $\{C_u, C_v\}$ of the periods C_u and C_v.
We now prove the further resultant $C_v \mid C_u$, whence it follows that $C_{uv} = C_u$.
For $n \geqq N_u$ from $(E^{C_u} - 1)u_n = 0$ it follows that

$$(E^{C_u} - 1)Vv_n = (E^{C_u} - 1)Uu_n = 0.$$

Further for $n \geqq N_v$ one has

$$(E^{C_v} - 1)v_n = 0.$$

Consequently for $n \geqq N = \max(N_u, N_v)$ one has $Gv_n = 0$, where G is the greatest common divisor of $(E^{C_u} - 1)V$ and $E^{C_v} - 1$. Now by condition III the resultant of V and $E^{C_v} - 1$ is equal to a constant $\neq 0$. Hence apart from a constant factor the polynomial G is equal to the resultant of $E^{C_u} - 1$ and and $E^{C_v} - 1$, i.e. to $E^d - 1$, where d denotes the greatest common divisor (C_u, C_v) of C_u and C_v.
By the minimum property of the primitive period C_v one concludes $C_v = d$, hence $C_v \mid C_u$.
Remark. If on U the supplementary condition is imposed that it be relatively prime to every cyclotomic polynomial, then by a similar argument one finds $C_u \mid C_v$, hence $C_u = C_v = C_{uv}$. In general we shall not assume this supplementary condition holds, consequently in general we have only

$C_v | C_u = C_{uv}$.

3. In order to deduce further properties we introduce the resultant M of the polynomials U and V. By condition II this resultant M is an integer $\neq 0$. By a property of resultants there exist polynomials X and Y with integer coefficients such that

(2) $\quad M = XU + YV.$

We now introduce the characteristic sequence (a) defined by

(3) $\quad a_n = Xv_n + Yu_n \qquad (n=0,1,\ldots)$

Then using (1) and (2) we have

(4) $\quad Ua_n = XUv_n + YUu_n = (XU+YV)v_n = Mu_n$

and similarly

(5) $\quad Va_n = XVv_n + YVu_n = (XU+YV)u_n = Mu_n.$

From (3) it follows that the sequence (a) is periodic and that $C_a | \{C_u, C_v\} = C_u$. Further from (5) it follows that

$$M(E^{C_a}-1)u_n = V(E^{C_a}-1)a_n = 0 \qquad (n=N_a, N_a+1, \ldots),$$

hence $C_u | C_a$ and consequently $C_a = C_u$. Thus the characteristic sequence (a) has the same period as the process.

Writing (4) in the form

$$Va_n \equiv 0 \pmod{M}$$

we learn that the sequence (a) reduced mod M satisfies a linear recurring relation with characteristic polynomial V.

Now under certain restrictions the period of the mod M reduced sequence is equal [1]) to $c(V,M)$. Here $c(V,M)$ denotes the smallest positive integer with

$$X^{c(V,M)} \equiv 1 \ (\text{modd } V(X), M).$$

These restriction are:

A. $V(0)$ and M are relatively prime;

B. The resultant of $\frac{V(E)-V(X)}{E-X} a_0$ and $V(X)$ is relatively prime to M.

Calling the prime factors of $V(0)$ and of the resultant of $\frac{V(E)-V(X)}{E-X} a_0$ and $V(X)$ exceptional for the considered reduced recurring sequence we may state the result in the following form.

If M has no exceptional prime factors the period c of the reduced recurring sequence is equal to the exponent $c(V,M)$. If however M possesses singular prime factors then the period c satisfies

$$c(V,M') \mid c \mid c(V,M),$$

[1]) Confer H.J.A.Duparc, Divisibility properties of recurring sequences, p.44-50, Thesis, Amsterdam 1953.

A shorter proof of this property will be given in the author's paper Periodicity properties of recurring sequences II, to appear in the Proc.Kon.Ned.Ak.van Wetensch. 1954.

where M/M' contains only exceptional prime factors.

Since C denotes the period of the sequence (a) and c denotes the period of the mod M reduced sequence (a) one has obviously $c \mid C$, hence under the conditions A and B

(6) $$c(V,M) \mid C.$$

In a similar manner from (4) one concludes

(7) $$c(U,M) \mid C,$$

if also for the sequence with characteristic polynomial U the integer M possesses no exceptional prime factors.

In the following sections some cases are considered in which more can be said then the results (6) and (7), in particular cases are treated where either $C=c(V,M)$ or $C=c(U,M)$. It is obvious that the first relation holds if one has $C \mid c$, i.e. if for sufficiently large n from $a_n \equiv a_{n+c} \pmod M$ it follows that $a_n = a_{n+c}$.

4. It is not difficult to find cases with $C=c(U,M)$. We show that these occur for instance if $V=m$ and M has no exceptional primes for the recurring sequence (a) with characteristic polynomial U.

In fact , in this case one has from (1) for $n=0,1,\ldots$

$$Uu_n = mv_n$$

and moreover

$$M=m,\ X=0,\ Y=1,\quad a_n=u_n.$$

Thus we get

$$Ua_n = mv_n\ ,\ \text{i.e.}\quad Ua_n \equiv 0 \pmod m.$$

Since by (1) one has $0 \leq u_n < m-1$ the sequence (u) is identical to the mod m reduced sequence (u) hence $C = c(U,M)$.

To this class of problems belong the recurring fractions, which are obtained when convertion the fraction u_o/m into the number system to the base p. Then one has

(8) $$pu_n = mv_n + u_{n+1} \qquad (n=0,1,\ldots).$$

It is not without interest to state here under what conditions m has no exceptional prime factors. The condition A requires $U(0)=p$ and m to be relatively prime, whereas condition B requires that

$$\frac{U(E)-U(X)}{E-X}\, u_o = u_o \quad \text{and m}$$

are relatively prime. Here one obtains the wellknown exceptional cases in the theory of recurring fractions.

The general kind of problems belonging to the case $m=V$, for which one has no longer necessarily $s=1$, is merely the theory of linear recurring sequences reduced mod m. For many properties of their periods $c(U,M)$ the reader is referred to the above mentioned papers.

In this section a further property on C could be given without

using the fact that the integers are ordered. Hence these results also hold if the elements of the sequence (u) do not belong to the residue set $0,1,\ldots,m-1 \mod m$ but belong to any arbitrary set of representants of the residue set mod m of the integers.[2] In the following section however I could not deduce the results without using the order of the positive integers.

5. We now consider cases where $C = c(V,M)$. As a first group of cases we take $V = mE-q$, where by property III we have $|q| \leq m-1$. Now (5) becomes

$$ma_{n+1} - qa_n = Mu_n \qquad (n = 0,1,\ldots).$$

Putting $a_{n+c}-a_n = Mb_n$, where as before c denotes the period mod M of the sequence (a) we get for sufficiently large n (and in this section unless stated otherwise only such n will be considered)

$$mb_{n+1} - qb_n = u_{n+c}-u_n.$$

(9) First we prove $|b_{n+1}| \leq |b_n|$.

In fact otherwise we would have $|b_{n+1}| \geq |b_n| + 1$, whence we would derive the contradiction

$$m-1 \geq |u_{n+c}-u_n| = |mb_{n+1}-qb_n| \geq m\,|b_{n+1}| - |qb_n| \geq m+(m-|q|)|b_n| \geq m.$$

Now first consider the case $q > 0$. Then one has $b_nb_{n+1} \geq 0$, for from $b_nb_{n+1} < 0$ we would obtain the contradiction

$$m-1 \geq |u_{n+c}-u_n| = |mb_{n+1}-qb_n| = m\,|b_{n+1}| + q\,|b_n| \geq m+q.$$

From the relation $c|C$ derived in section 3 we get putting $C = rc$ and using the definition of b_n

$$(10) \qquad 0 = a_{n+rc}-a_n = M(b_n+b_{n+c}+\ldots+b_{n+(r-1)c}),$$

hence $b_n = 0$ and $a_{n+c} = a_n$, i.e. $c = C$.

Further consider the case $q < 0$. Then one has

$$(11) \qquad b_nb_{n+1} \leq 0,$$

for from $b_nb_{n+1} > 0$ we would obtain the contradiction

$$m-1 \geq |u_{n+c}-u_n| = |mb_{n+1}-qb_n| = m\,|b_{n+1}| + |qb_n| \geq m+q.$$

If c is even we use the relation (10), which also holds in this case. Then we conclude as before $b_n = 0$ i.e. $c = C$.

[2]) Consequently the above results hold also for sequences the elements of which belong to the more general ff-sets, introduced in the above mentioned papers.

If however c is odd we use the relation

$$0 = a_{n+2rc} - a_n = M(b_n + b_{n+c} + \ldots + b_{n+(2r-1)c});$$

herefrom using (9) and (11) it follows that $b_n + b_{n+c} = 0$, hence $a_{n+2c} = a_n$, i.e. $C = 2c$.

The case $U = 1-E^2$, $V = 3E+2$ with $M = 5$, $c = 1$, $C = 2$ shows that $C = 2c$ can occur.

Also in another class of cases we can prove $c = C$, viz. in the cases $V = mE^t \pm 1$.

If $V = mE^t - 1$, then (5) becomes for $n = 0,1,\ldots$

$$(12) \qquad (m E^t - 1)a_n = Mu_n,$$

hence

$$(m^r E^{rt} - 1)a_n = M \sum_{j=0}^{r-1} m^j E^{jt} u_n,$$

consequently

$$0 \leqq m^r a_{n+rt} - a_n \leqq M(m-1) \sum_{j=0}^{r-1} m^j = M(m^r - 1),$$

$$\frac{a_n}{m^r} \leqq a_{n+rt} \leqq M + \frac{a_n - M}{m^r},$$

hence if h is sufficiently large

$$1 \leqq a_h \leqq M,$$

provided $a_h \neq 0$.

From (12) for $a_n = 0$ one deduces $a_{n+t} = 0$ on account of $0 \leqq u_n \leqq m-1$. (Similarly from $a_n = M$ one deduces $a_{n+t} = M$).

If $a_n \neq 0$, $a_n \neq M$ from $a_{n+c} \equiv a_n \pmod M$ one concludes $a_{n+c} = a_n$ and $C = c$.

Here one has $X^t \equiv 1/m \pmod{V(X)}$,

hence if e denotes the exponent of m mod M one has $X^{et} \equiv 1 \pmod{V(X), M}$ and it is not difficult to prove the et is the smallest positive exponent with this property. 3)

Consequently $C = et = tc_m(M)$ and this holds also if some elements of the sequence (a) are equal to 0 or to M.

If $V = m E^t + 1$, then we get similarly

$$(m^r E^{rt} - (-)^r)a_n = M \sum_{j=0}^{r-1} (-)^{r-1-j} m^j E^{jt} u_n,$$

---

3) H.J.A. Duparc, loc.cit. theorem 45, p.40.

consequently

$$(-)^r a_n - M\, m^r \frac{m-1}{m^2-1} \leqq m^r\, a_{n+rt} \leqq (-)^r a_n + M\, m^{r+1} \frac{m-1}{m^2-1},$$

hence for sufficiently large r

$$-M \frac{m-1}{m^2-1} \leqq a_{n+rt} \leqq M \frac{m(m-1)}{m^2-1}.$$

Since the difference of the left and righthand side of this relation is equal to M for sufficiently large h from $a_{h+c} \equiv a_h \pmod M$ one deduces $a_{h+c} = a_h$ and $C = c$, provided one of the exceptional cases $a_h = \frac{-M}{m+1}$ or $\frac{mM}{m+1}$ holds. Since from $a_h = \frac{mM}{m+1}$ it follows $a_{h+t} = \frac{-M}{m+1}$ and conversely, we get for even $e' = e_{-m}(M)$ the result $C = c$ and for odd e' the result $C = 2c$.

6. Very simple applications of the results of the preceding section occur for linear U and V, say

$$U = E+p,\ V = mE-q. \qquad (0 < q < m).$$

These processes can be considered as an immediate generalisation of those on recurring fractions given in section 4, formula (8).

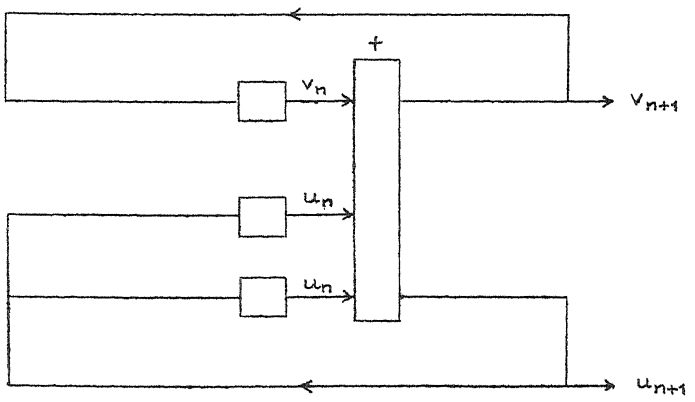
Here one has $M = |mp+q|$. The condition A here requires that q and M are relatively prime, i.e. that $(q,mp) = 1$; the condition B requires $(m\, a_0, M) = 1$. We assume these conditions satisfied, i.e. $(q,m) = (q,p) = (a_0,M) = 1$.

Here V is linear, hence the period $c(V,M)$ is equal to the exponent of $\frac{q}{m} \bmod M$ which will be denoted by $e_{q/m}(M)$. Then also the period of the process is equal to this number.

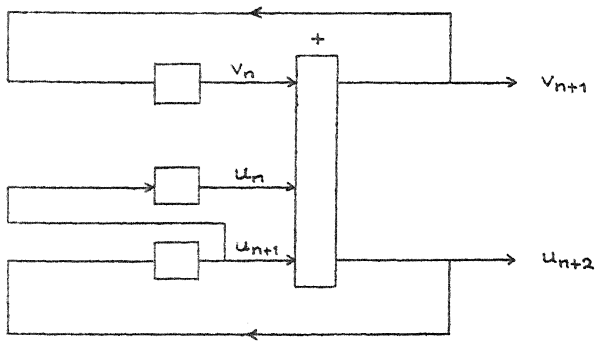
The process is given by the recurring equation

$$pu_n + qv_n = u_{n+1} + m\, v_{n+1} \qquad (n = 0,1,\ldots),$$

which can easily be represented by a cyclic computing circuit, which works in the number system to the base m. We show below the case $p = 2$, $q = 1$.



Another interesting circuit is given by the computing network



The corresponding equation is

$$u_n+u_{n+1}+v_n = u_{n+2}+m\ v_{n+1} \qquad (n = 0,1,\ldots).$$

Here

$$U = -E^2 + E+1,\ V = mE-1,\ M = m^2 + m-1$$

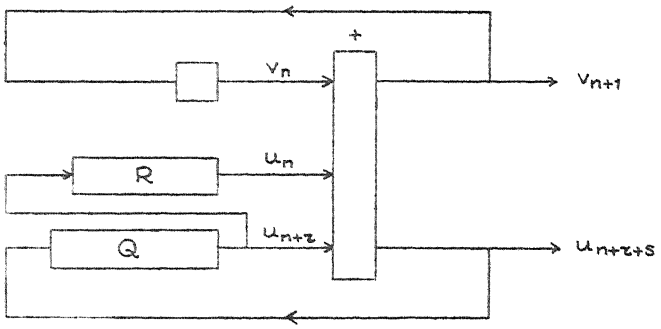
and the condition A is obviously satisfied. The condition B requires $(a_o,\ m^2+m-1)= 1$. Supposing B holds one has

$$C = c_m\ (m^2+m-1).$$

As a last example we take the process

$$u_n+u_{n+r}+v_n = u_{n+s} + m\ v_{n+1} \qquad (n=0,1,\ldots;0 \leq r < s),$$

realised by the computing network



Here Q and R denote delay lines with length $q = s-r > 0$ and r respectively. We have

$$U = 1 + E^r - E^s,\ V = m\ E-1,\ M = m^s + m^{s-r} -1.$$

Since $V(0)= -1$ the condition A holds; the condition B holds if we assume ma_o and M, i.e. a_o and M relatively prime. Then one finds

$$C = c_{1/m}\ (M)= c_m\ (m^s + m^q - 1).$$