ON THE PERIOD OF PSEUDO-RANDOM NUMBERS GENERATED BY LEHMER'S CONGRUENTIAL METHOD

SHINICHI YAMADA

Nippon Remington Univac Kaisha, Ltd.

(*Received Sept. 11. 1959*)

It is well known that a sequence of randon numbers may be generated by Lehmer's congruential method. This method was originally executed in the formula;

$$x_{n+1} \equiv 23x_n \pmod{10^8+1}.$$

The period of this sequence comes up to 5, 882, 352 which seems to be sufficient for almost all of our applications. The purpose of this paper is to provide an elementary method to account such a period of pseudo-random numbers generated by Lehmer's method.

1. CONGRUENTIAL METHOD

At first we define congruential method (multiplicative).

Definition: Congruential method (multiplicative) is the method of generating sequences of integers in the following way.

Take a triple of positive integers (M, k, x_0), and get a sequence of integers by relation;

$$x_{n-1} \equiv kx_n \pmod{M}.$$

When generating a sequence (x_i) following the above relation, if for some integer N, x_N is equal to x_0, then x_{+1} is equal to x_1 and x_{N+2} is equal to x_2 and so on, therefore significant section of this sequence, that is, the section which contains whole of the mutually distinguished integers, is $(x_1, x_2, \cdots\cdots, x_N)$.

So, when we apply this method to get random numbers uniformly distributed on the unit interval, it is sufficient to repeat the process of generation up to N times, if the results of test were sufficiently fit for our purpose.

Hence we define the period of sequence (x_i) as follows:

Definition: The period of the sequence (x_i) is the minimal element of the set (n_i) of positive integers, each element n_i of which satisfies

the equation $x_{ni}=x_0$,
i. e.

$$(n_i)=(n_i\,;\ i\epsilon I,\ x_{ni}=x_0,\ \text{for all } n_i,\ n_i>0).$$

Here I is an indexing set composed of zero and positive integers.

Remark: In triple $(M,\ k,\ x_0)$, if $x_0\equiv 0 \pmod M$ or $k\equiv 0 \pmod p$ for any prime disvisor p of M, we call it a trivial triple. (Meaning of "trivial" is clear in the sense that, if triple is trivial, generated sequence has no adequate significant section.)

In reality, trivial triple is not worth cutting figure for our object of consideration, from the results of randomness, too.

In the above definition of the period, we preassumed the existence of the set (n_i) of positive integers, but in the next lines, I prove the existence theorem;

Existence Theorem: For all non-trivial triples $(M,\ k,\ x_0)$, there exist the period.

Proof: For the existence of the set of integers (n_i), it is sufficient to prove the existence of a positive integer n' such that $x_{n'}=x_0$.

By the relation $\quad x_{n+1}\equiv kx_n \pmod M$,
the above statement is equivalent to

$$\exists n'\,;\ (k^{n'}-1)\ x_0\equiv 0 \pmod M$$

As triple $(M,\ k,\ x_0)$ is not trivial, $(x_0,\ M)=d\neq M$,

$$\text{therefore} \quad k^{n'}-1\equiv 0 \pmod{M/d}.$$

Now, the existence of n' is clear, if we assign $n'=\varphi\,(M/d)$ where φ is Euler's function.

i. e. by $k\not\equiv 0 \pmod M$, $\quad k^{\varphi(d/M)}\equiv 1 \pmod{M/d}$. ——Fermat's theorem,[1]
therefore, the existence of period is proved.

2. ACCOUNT OF PERIOD

Now, let $(M,\ k,\ x_0)$ be a non-trivial triple and get the sequence (x_i) by the relation $x_{n+1}\equiv kx_n \pmod M$, and the period of this sequence be N.

i. e. $\quad N=\min\,(n_i\,;\ x_{ni}=x_0)$,
if one writes the relation in the following way,

$$(x_0,\ M)=d,\quad k^{\lambda}-1\equiv 0 \pmod{M/d}$$

1 See Appendix 1.

we obtain $N=\min(\lambda;\ k^{\lambda}-1\equiv 0 \pmod{M/d})$.

Definition: Period of k mod M/d is the minimal element N which satisfies the relation $k_N-1\equiv 0 \pmod{M/d}$.

Decompose M/d into prime divisors; $M/d=\prod_i^r p_i^{e_i}$,

then one gets the following isomorphism,

$$Z/(\prod_i^r p_i^{e_i})\approx\sum_i^r Z/(p_i^{e_i}), \qquad \text{(direct)}^1$$

here, Z is the *additive group of integers.*

Therefore, if we get the period N_i of k for all p_i, then, desired period N is equal to the least common multiple $\{N_1, N_2, \cdots\cdots N_r\}$.

The above isomorphism is just the fundamental theorem of abelian group.[1]

This can be explained as follows:

Let Z be the additive group of integers and let f_i be homomorphism of Z into Z defined as follows:

$$z\epsilon Z,\ f_i(z)=p_i^{e_i}z,$$

then, the sequence

$$0\longrightarrow Z/(\prod_i^r p_i^{e_i})\xrightarrow{f_i} Z/(\prod_i^r p_i^{e_i})\xrightarrow{h}(Z/\prod_i^r p_i^{e_i})/p_i^{e_i}(Z/\prod_i^r p_i^{e_i})\longrightarrow 0$$

is exact and split. (h is natural homomorphism.)

Therefore, inductively, we get the relation

$$Z/(\prod_i^r p_i^{e_i})\approx\sum_i^r Z/(p_i^{e_i}) \qquad \text{(direct)}$$

and then, N_i is an order of k in $Z/(p_i^{e_i})$.

So we get the relation.

$$N=\{N_1, N_2, \cdots\cdots, N_r\}.$$

Hence, the account of period is reduced to the following problem.

Problem: Calculate minimal (positive) integer N, which satitfies the relation: $k^N-1\equiv 0 \pmod{p^{\lambda}}$ for p prime.

When the primary decomposition of M/d (in Z) contains primary divisor 2^{λ}, $\lambda\geqslant 3$, we first calculate the period of k mod p^{λ} in the case $p\neq 2$, for the structure of $Z/(2^{\lambda})$ is a bit singular.

(i) $p\neq 2$

Let m be the period of k mod p i. e. $m=\min(\lambda';\ k^{\lambda'}\equiv 1 \pmod{p})$ and let desired period of k mod p^{λ} be N, then, by the relation,

$$k^N \equiv 1 \pmod{p^\lambda}, \text{ naturally, } k^N \equiv 1 \pmod{p},$$

m is the period of k mod p, therefore m/N, i. e. m is a divisor of N.

On the other hand, $k^{\varphi(p^\lambda)} \equiv 1 \pmod{p^\lambda}$ and N is the period of k mod p^λ, so N is a divisor of $\varphi(p^\lambda) = p^{\lambda-1}(p-1)$.

As the result, we can write down in the following form,

$$N = m \cdot n' \cdot p^{\lambda-\alpha}\,;\ n' | p-1,\ \alpha \geqslant 1.$$

Lemma: let $p^h || k^m - 1$, then $p^{h+r} || k^{mp^r} - 1$, for each positive integer r[2].

proof:

$$p^h || k^m - 1 \longrightarrow \exists v\,;\ k^m = 1 + p^h v,\ (v,\ p) = 1,$$

then $k^{mp} = (1 + p^h v)^p = 1 + p^{h+1} v + \binom{p}{2} v^2 p^{2h} + \cdots\cdots$

$$= 1 + p^{h+1}(v + pu).$$

by $(v,\ p) = 1$, $p^h || k^{mp} - 1$,

inductively, we get the above proposition.

By this Lemma, we get, $p^{h+\lambda-\alpha} || k^{mp^{\lambda-\alpha}} - 1$

On the other hand, $k^N = k^{m \cdot n' \cdot p^{\lambda-\alpha}} = (1 + p^{h+\lambda-\alpha}(v + pu'))^{n'}$, $(v,\ p) = 1$,

$$= 1 + p^{h+\lambda-\alpha}(n'v + pu), \text{ and } n' | p-1.$$

$$\therefore \quad (n',\ p) = 1,\ (n'v,\ p) = 1,$$

$$p^{h+\lambda-\alpha} || k^N - 1.$$

Now if $n' = 1$, then $N' = mp^{\lambda-\alpha}$ is strictly smaller than N, and that contradicts the hypothesis that N is minimal.

Therefore, $n' = 1$.

On the other hand $p^{h+\lambda-\alpha} || k^N - 1$, i. e. $p^\lambda | p^{h+\lambda-\alpha}$,

hence $h \geqslant \alpha$.

Here, if h is strictly larger than α, then $p^h || k^m - 1$, and therefore, $p^{h+(\lambda-h)} || k^{mp^{\lambda-h}} - 1$ by the relation $mp^{\lambda-h} < mp^{\lambda-\alpha}$.

This contradicts the hypothesis that N is the peried of k mod p^λ. (minimal !)

$$\therefore \quad h = \alpha$$

Hence, we get the following proposition which combines N and the pair $(m,\ h)$

proposition: The period N of k mod p^λ is written in the following way,

2 See Appendix 2.

$$N=mp^{\lambda-h},$$

here, m is the period of k mod p and h is the integer such that p^h divides strictly k^m-1, i. e. $p^h||k^m-1$.

Note: The case $h>\lambda$ does not occur.

With this proposition, it is comparatively easy to calculate the period N, for the problem is reduced to the case in prime divisors.

That is, if we find primitive root for each prime divisor p, we can obtain the period of k with respect to p^λ in extremely easy way and alternatively, if we take primitive root of each primary divisor, for k, it is possible to get relatively long significant section and if M/d is primary, we will get the longest significant section.

(ii) Account of the period of k mod 2^λ

In the case $\lambda=1$ or 2, $Z/(2^\lambda)$ is cyclic, hence the above proposition is available, but, shown in the following, this case is trivial and impractical.

$\lambda=1$, $Z/(2)$ is composed of two residue class (even, odd) and $\varphi(2)=1$

hence, $k\epsilon$ (odd) $\longrightarrow$ $N=1$

$k\epsilon$ (even) $\longrightarrow$ this triple is trivial.

$\lambda=2$ $\varphi(2^2)=2$, primitive root is 1

hence, $k=-1+4u \longrightarrow N=2$

$k=(-1)^2+4u \longrightarrow N=1$

k; even $\longrightarrow$ triple is trivial.

Therefore, we calculate the period of k mod 2^λ for $\lambda\geqslant 3$.

As period N is a divisor of $\varphi(2^\lambda)$, N will be written in the form 2^α, $\alpha\leqslant\lambda-1$.

Hence if we find maximal integer e that satisfies the relation $k=\pm 1+2^e v$, $(2, v)=1$, which will be found with ease, after the verification whether k is congruent with $+1$ or with -1 modulo 4.

then $k^N=k^{2^\alpha}=(\pm 1+2^e v)^{2^\alpha}=1\pm 2^{e+\alpha}(v+2M)$

Hence $2^{e+\alpha}||k^N-1$

By the hypothesis that $k^N-1\equiv 0 \pmod{2^\lambda}$,

$$2^\lambda|2^{e+\alpha}||k^N-1$$

$$\therefore \quad e+\alpha\geqslant\lambda, \text{ i. e. } \alpha\geqslant\lambda-e.$$

As N is the period, it is minimal.

$$\alpha=\lambda-e$$

$$\therefore \quad N=2^{\lambda-e}$$

If we scrutinize a little the structure of $Z/(2^\lambda)$ for $\lambda \geqslant 3$, the reason why we can obtain the period by the process mentioned above will be clarified.

For $\lambda \geqslant 3$, $Z/(2^\lambda)$ is identified with the direct product of cyclic group of order 2 and cyclic group or order $2^{\lambda-2}$, and $<-1, 5>$ will be taken for its basis.

Therefore, one half of the reduced residue classes in quotient ring $Z/(2^\lambda)$ and another half are represented in the form $(-1)^2 \cdot 5^u$ for $u=0, 1, 2, \cdots\cdots \varphi(2^\lambda)/2-1$, and $(-1) \cdot 5^{u'}$ for $u'=0, 1, \cdots\cdots \varphi(2^\lambda)/2-1$ respectively, and the former set of classes represents the class of odd numbers in the form $4n+1$, and the latter the class of odd-numbers in the form $4n-1$ for some integer n, and which is clear by the equality $5=1+2^2$

The choice of representation $k=1+2^e v$ or $k=-1+2^e v$ follows from these structure of $Z/(2^\lambda)$; that is, if k is written in the form $1+2^e v$, (e, max), then k is contained in the former set of classes and represented to be $(-1)^2 \cdot 5^u$ for some u, and if written in the form $-1+2^e v$, (e, max), then k is contained in the latter set of classes and represented to be $(-1) \cdot 5^u$ and conversely.

From these fact, by classification of k modulo 4, maximal integer e will be found easier.

Simple "inductive" method described above will provide us the desired results by simple calculation and, conversely, it is quite easy to choose a triple for desired scale of the significant section.

3. EXAMPLES

By the method described above, I will calculate the periods, and test the result for various examples in "Symposium" (1954) and give a bit of criticism.

(1) Example which was run on ENIAC by Lehmer.

He used the relation $x_{n+1} \equiv 23 x_n \pmod{10^e+1}$ and generated the sequence of 8-decimal numbers, of which period was known to be 5882352.

(Account)

Let N be the period, that is, the minimal element which satisfies the relation $23^N-1 \equiv 0 \pmod{10^8+1}$ and consider the decomposition of 10^8+1

$$10^8+1=17\times 5882353,$$

then the period of 23 mod 17 will be found immediately equal to $\varphi(17)=16$, for 23 is a primitive root of 17. Without table of prime numbers, it is not sure, but probable that 5882353 is prime and 23 is a primitive root of 5882353.

Under the assumption that 5882353 is prime, the period of 23 mod 5882353 is $\varphi(5882353)=5882352$.

(2) Example on SEAC by Cameron in 1950

(Account) $x_0=1,\ x_{n+1}\equiv 15^{17}x_n \pmod{2^{42}}$

$5\equiv 1 \pmod 4$

therefore $5^{17}=1+17\cdot 2^2+\binom{17}{2}\cdot 2^4+\cdots\cdots$

$=1+2^2(1+2M)$

and $(1+2M,\ 2)=1,$

$\therefore\quad e=2$

Here $\lambda=42$, we obtain $N=2^{42-2}=2^{40}$.

(3) Example on SWAC by Teichoew

$$x_0=1,\ x_{n+1}\equiv 5^{13}x_n \pmod{2^{36}}$$

Generalizing this relation, I give here the period of sequences generated by relation

$$x_0=1,\ x_{n+1}\equiv 5^{2h+1}x_n \pmod{2^\lambda}$$

(Account)

$$5^{2h+1}=(1+2^3(1+2M')^h\cdot(1+2^2)$$
$$=1+2^2(1+2M'')$$

therefore $e=2.$

Hence, in general, $N=2^{\lambda-2}$

for $\lambda=31,\ N=2^{34}$.

In other examples, for instance, those on ORDVAC, EDVAC, results are good.

Remark: In the above example, k is taken to be 5^{2h+1}, which I consider is due to fact that order of 5 is maximal in $Z/(2^\lambda)$ and equal to $2^{\lambda-2}$.

[Example on decimal machines]

(4) Example on OARAC

$$x_0=1,\quad x_{n+1}\equiv 7x_n \pmod{10^{10}}$$

(Account)

Let N' be the period of 7 mod 2^{10} and N'' be the period of 7 mod 5^{10}, then desired period N is equal to $\{N', N''\}$.

(N'): $\quad 7\equiv-\ (\mathrm{mod}\ 4) \qquad 7=-1+2^3$

$$\therefore \quad N'=2^{10-3}=2^7$$

(N''): First, we calculate the period m of mod 5

$7\equiv 2(\mathrm{mod}\ 5)$ and 2 is a primitive root of 5.

$$\therefore \quad m=\varphi(5)=4$$

Next, we calculate h such that $5^h||7^4-1$

$$7^4-1\equiv 2^5\cdot 3\cdot 5^2 \qquad \therefore \quad k=2$$

therfore $\quad N''=5^8\cdot 4 \qquad \therefore \quad N=\{2^7,\ 5^8\cdot 4\}=5\times 10^7$

(5) Example fit for UNIVAC

$$x_0=1,\quad x_{n+1}\equiv 7^{4k+1}x_n\ (\mathrm{mod}\ 10^{11}) \quad k:\ \text{integer.}$$

In Taussky and Todd's paper, it is written that the period of sequence by this relation is 5×10^8

(Account)

Let N' be the period of 7^{4k+1} mod 2^{11} and N'' be the period of 7^{4k+1} mod 5^{11}.

(N'): $\quad 7\equiv -1\ (\mathrm{mod}\ 4)$

$$\therefore \quad 7^4{}_k{}^{+1}=-1+(4k+1)2^3-\binom{4k+1}{2}\cdot 2^6+\cdots\cdots$$

$$=-1+2^3(1+2M)$$

$$\therefore \quad N'=2^{11-3}=2^8.$$

(N''): First we calculate the period m of 7^{4k+1} mod 5

$7\equiv 2$ mod 5

and $(2^{4k+1})^m-\equiv 2^m-\equiv 0\ (\mathrm{mod}\ 5)$

$$\therefore \quad m=\varphi(5)=4.$$

Next, we calculate h, similarly.

$$(7^{4k+1})^4-1=(49^{4k+1}-1)(49^{4k+1}+1)$$

As $49^{4k+1}-1$ is congruent with 3 mod 5

$$5^k||(50-1)^{4k+1}+1$$

$$(50-1)^{4k+1}+1=(4k+1)\cdot 5^2\cdot 2-\binom{4k+1}{2}\cdot 5^4\cdot 2^2+\binom{4k+1}{3}\cdot 5^6\cdot 2^3-\binom{4k+1}{4}\cdot 5^3\cdot 2^4$$
$$+\binom{4k+1}{5}\cdot 5^{10}\cdot 2^5+5^{12}\cdot M$$

In the above relation, if $4k+1\not\equiv 0$ (mod 5), that is, $k\not\equiv 1$ (mod 5), then, $5^2||(50-1)^{4k+1}+1$,

$$\therefore \quad h=2.$$

Hence $N''=5^{11-2}\cdot 4$

$$\therefore \quad N[2^8,\ 5^9\cdot 4]=5\times 10^8.$$

On the other hand, if $4k+1\equiv 0 \pmod 5$, the period will vary extremely. It is shown in the following, (in this case, triples are trivial).

$$\begin{aligned}(50-1)^{4k+1}+1=&(4k+1)\cdot 5^2\cdot 2-4k\cdot(4k+1)\cdot 5^4\cdot 2^2\\ &+8/3\cdot k(4k+1)(4k-1)\cdot 5^6\cdot 2\\ &-8/3\cdot k(4k+1)(4k-1)(4k-2)5^8\\ &+16/3\cdot k(4k+1)(4k-3)(4k-2)\cdot 5^9\\ &\qquad\qquad\qquad\qquad\qquad\qquad \pmod{5^{11}},\end{aligned}$$

therefore, in the case $h-2\leqslant\lambda=11$, i. e. $k\leqslant 9$.

We reduce the above relation with use of relation $4k+1\equiv 0 \pmod 5$ in the following way.

Let k_0 denote k_1,

$4k_0+1\equiv 0 \pmod 5$, $\Rightarrow \exists\ (k_1,\ u_1)$; $k_0=1+k_1\cdot 5^{u_1}$, $(k_1,\ 5)=1$,

Now,

(1, 1) $\quad u_1\geqslant 2$ or $u_1=1$, $k_1\not\equiv 1 \pmod 5$

$5\|4k+1$, $\quad\therefore\ N''=5^{9-1}\cdot 4=5^8\cdot 4 \quad\therefore\ N=10^8$

$\because)\ \ 4k+1=4(1+k_1 5^{u_1})+1=5(1+4k_1 5^{u_1-1})$

if $u_1\geqslant 2$, then, $1+4k_1\cdot 5^{u_1-1}\not\equiv 0 \pmod 5$

if $u_1=1$, $k_1\not\equiv 1 \pmod 5$, then $4k_1+1\not\equiv 0 \pmod 5$

(1, 2) $\quad u_1=1$, $k_1\equiv 1 \pmod 5$

$\Rightarrow \exists\,(k_2,\ u_2)$; $k_1=1+k_2\cdot 5^{u_2}$, $(k_2,\ 5)=1$,

let's continue the process similar to (1, 1),

(2, 1) $\quad u_2\geqslant 2$, or $u_2=1$, $k_2\not\equiv 1 \pmod 5$

$5^2\|4k+1$, $\quad\therefore\ N''=5^7\cdot 4 \quad\therefore\ N=5^7\cdot 2^8$,

we obtain analogously,

$(n,\ 2)$ $\quad u_n=1$, $k_n\equiv 1 \pmod 5$

$\Rightarrow \exists\ (k_{n+1},\ u_{n+1})$; $k_n=1+k_{n+1}\cdot 5^{u_{n+1}}$

$(n+1,\ 1)$, $u_{n+1}\geqslant 2$, or $u_{n+1}=1$, $k_{n+1}\not\equiv 1 \pmod 5$

$N''=5^{8-n}\cdot 4 \qquad\therefore\ N=5^{8-n}\times 2^8$.

Hence, collect and arrange the results obtained above, we obtain the following relation, or in another word, dependency of periods on triples.

1° $\quad k\not\equiv 1 \pmod 5 \quad\Rightarrow\ N=5\times 10^8$

2° $\quad k\equiv 1 \pmod 5$

$$\left.\begin{array}{ll} k=1/4\cdot(5^n-1)+k'5^{u+n-1}, & u\geqslant 2 \\ \text{or} \quad k=1/4(5^n-1)+k''5^n, & k''\not\equiv 1(\text{mod } 5) \end{array}\right\} \begin{array}{l} N=2^8\cdot 5^{9-n} \\ (1\leqslant n\leqslant 9) \end{array}$$

Thus, in accordance with these practical situation, it may be rather fit for reality that we choose a triple satisfying for the relation $k\not\equiv 1$(mod 5) in the above example; in the worst case, i. e. in the case $k=(5^9-1)/4$ obtained significant section in sequence of "pseudo-random" numbers consists of only 256 numbers.

Criticism: In this example, k is taken to be 7^{4k+1}, and that is considered because $7=2+5$ is nothing but a primitive root of $5^u\cdot 2$ $(n\geqslant 1)$ and provides comparatively long significant section, but here, note that 3 is also a primitive root of 5 and relatively prime to 2^λ for $\lambda\geqslant 1$, in the case when we assign 3^{4k+1} to k and use a triple $(10^m, 3^{4k+1}, 1)$, $k\not\equiv 1$ (mod 5) for generation, it is certain that we get as long sequence as that in the above example and generated sequnce will be useful,, if its random qualities were tested to be satisfactory:

For, let $x_0\not\equiv 0$ (mod 2), and $x_0\not\equiv 0$ (mod 5) and generate the sequence by the relation

$$x_{n+1}\equiv 3^{4k+1}x_n \text{ (mod } 10^m) \text{ and } k\not\equiv 1 \text{ (mod 5)}$$

The period, in the case $m\geqslant 3$, will be $2^{m-2}\cdot 5^{m-1}=5\times 10^{m-2}$.

APPENDIX

(1) For the proof of this theorem, it is sufficient to prove the following theorem.

Theorem: Let p and q be relatively prime positive integers, i. e.

$(p, q)=1$, and let N_p and N_q be the period of k mod p and mod q respectively, then the period N of k mod pq is equal to the least common multiple of N_p and N_q.

Proof: If $k^m-1\equiv 0$ (mod p), i. e. $\exists v$; $k^m=1+v\cdot p$ then, by assumption on the period, N_p divides m, as N_p is the minimal positive integer of these.

Moreover, if $k_m-1\equiv 0$ (mod q), i. e. $\exists v'$; $k^m=1+v'\cdot q$, then it is also true that N_q divides m.

Hence, for $pq|k^m-1$, it is necessary that $p|k^m-1$, and $q|k^m-1$ and, therefore, m must be a common multiple of N_p and N_q.

Hence by minimality assumption on N, N is equal to the least common multiple.

(2) $p|q$ means p divides q in Z, i. e. $q=a\times p$ for some integer a,
$p^h||q$ means $p^h|q$ and $p^{h+1}|q$.

REFERENCE

[1] Van ber Waerden, Modern Algebra I, II.
The above examples are quoted from:
O. Taussky & J. Todd, "Generation and testing of pseudo-random numbers," Symposium on Monte Carlo Methods, University of Florida, 1954, John Wiley and Sons, Inc.,

The paper title below is beyond my hand, and it is my regret that I couldn't see Duparc, Lekkerkerker and Peremant' report.

H. J. A. Duparc, C. G. Lekkerkerker, and W. peremans:
"Reduced sequences of integers and pseudo-random numbers."
Math. Centrum, Report ZW 1953-002.

I take this opportunity of thanking Prof. Sekine and Mr. Yamasaki for their recommendation.