A NOTE ON SEMI-SPECIAL PERMUTATIONS

by K. R. YACOUB

(Received 4th November, 1957)

In a recent paper [1], the theory of non-linear semi-special permutations has been developed. A method for describing such permutations, on a given range $[n]$, is to be found in §§ 2, 3. This method consists in choosing a proper divisor s of n, determining all the semi-special permutations with principal number s, and then making s take all its possible values. In this way the totality of non-linear semi-special permutations on $[n]$ may be obtained.

Further, if π is a semi-special permutation with principal number s, then (see [1, Definition 2.4]) π induces modulo s a linear permutation. Accordingly the permutations with principal number s were divided (see [1], § 3) into two classes: the first class consists of the permutations which induce modulo s the identity permutation; while the second consists of those permutations which induce modulo s linear permutations other than the identity. The question arises whether permutations of the same class, or possibly of different classes (though with different values of the parameter s), can be identical. It is the object of the present note to answer this question.

Another question, closely related to the stated one, also arises, namely, whether one of the classes just considered is perhaps a sub-class of the other.* The answer to this question is in a few known cases affirmative (Cf. [2, §§ 4, 5]); but in general the author has no complete answer.

1. Preliminary results

THEOREM 1. (i) *If there is a non-linear semi-special permutation π on $[n]$ with principal number s and if π induces modulo s the identity permutation, then π can be written in the form*

$$\pi x \equiv x + s\lambda(1 + \omega + \ldots + \omega^{x-1}) \pmod{n}, \qquad \ldots\ldots\ldots\ldots(1)$$

where λ is prime to N, $N = n/s$, and where

$$\omega^s - 1 \equiv 0 \pmod{N}, \qquad \omega - 1 \not\equiv 0 \pmod{N}. \qquad \ldots\ldots\ldots\ldots(2)$$

(ii) *Conversely, if λ is prime to N, and ω satisfies* (2), *then* (1) *defines a non-linear semi-special permutation of the desired type* [1, Theorem 3.1].

THEOREM 2. (i) *If there is a non-linear semi-special permutation π on $[n]$ with principal number s, if π induces modulo s a linear permutation other than the identity and if $\pi 1 = t$, then t is prime to n and π can be written in the form*

$$\pi x \equiv tx + s\psi(x) \pmod{n} \qquad \ldots\ldots\ldots\ldots(3)$$

with $\psi(1) \equiv 0 \pmod{N}$, $\psi(x) \equiv R \sum_{i=1}^{x-1} (x-i)\theta^{i-1} \pmod{N}$ *for* $x \geqslant 2$, $\qquad \ldots\ldots\ldots\ldots(4)$

where R is prime to N, $N = n/s$, and

$$1 + \theta + \ldots + \theta^{s-1} \equiv 0 \pmod{N}. \qquad \ldots\ldots\ldots\ldots(5)$$

* This question was pointed out to the author by the referee.

https://doi.org/10.1017/S2040618500033657 Published online by Cambridge University Press

Moreover, if h is the order of t modulo s and u is defined modulo N by $t^h \equiv 1 + us \pmod{n}$, then

$$u + \sum_{i=0}^{h-1} t^{h-i-1}\psi(t^i) \quad \textit{is prime to } N\,; \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(6)$$

$$u(\theta - 1) \equiv \sum_{i=0}^{h-1} t^{h-i-1}\{\psi(2t^i) - (\theta+1)\psi(t^i)\} \pmod{N}\,; \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(7)$$

$$\sum_{i=0}^{h-1} t^{h-i-1}(1 + \theta + \ldots + \theta^{ti-1})^2(\theta^{rt^i} - \theta^r) \equiv 0 \pmod{N} \quad (r = 1, 2, \ldots, s). \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(8)$$

(ii) *Conversely, if t is prime to n and R is prime to N and if θ, t and R satisfy* (5)–(8), *then* (3) *defines a non-linear semi-special permutation of the desired type* [1, Theorem 3.10].

The permutation π, described in Theorem 1, is of the first class; it depends on three parameters, namely s, λ and ω; for this reason it may be denoted by $\pi(s\,;\ \lambda,\ \omega)$. But the permutation π of Theorem 2 belongs to the second class; it depends on four parameters, namely s, t, R and θ, and may be denoted by $\pi(s\,;\ t,\ R,\ \theta)$. The parameters s and t are to be determined modulo n, whilst R, λ, ω and θ are to be determined modulo N, where $N = n/s$. We use throughout s and s' for proper divisors of n and put $N = n/s$, $N' = n/s'$.

2. The main results

LEMMA 1. *$\pi(s'\,;\ \lambda',\ \omega') = \pi(s\,;\ \lambda,\ \omega)$ if and only if*

$$s' = s, \quad \lambda' \equiv \lambda \pmod{N}, \quad \omega' \equiv \omega \pmod{N}.$$

For if $\pi(s'\,;\ \lambda',\ \omega') = \pi(s\,;\ \lambda,\ \omega)$, then (see Theorem 1, (1))

$$s'\lambda'(1 + \omega' + \ldots + \omega'^{x-1}) \equiv s\lambda(1 + \omega + \ldots + \omega^{x-1}) \pmod{n}, \text{ for all } x. \qquad \ldots\ldots\ldots\ldots\ldots\ldots(9)$$

For $x = 1$, we have

$$s'\lambda' \equiv s\lambda \pmod{n}, \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(10)$$

and therefore $(s'\lambda',\ s'N') = (s\lambda,\ sN)$; but since $(\lambda,\ N) = 1$ and $(\lambda',\ N') = 1$, it follows that $s' = s$ and hence, by (10), $\lambda' \equiv \lambda \pmod{N}$. Furthermore, if we put $x = 2$ in (9) and use (10), we find that $\omega' \equiv \omega \pmod{N}$. This proves the necessity of the conditions of the lemma. The sufficiency of the conditions is trivial.

LEMMA 2. *$\pi(s'\,;\ t',\ R',\ \theta') = \pi(s\,;\ t,\ R,\ \theta)$ if and only if $s' = s$, $t' \equiv t \pmod{n}$, $R' \equiv R \pmod{N}$, and $\theta' \equiv \theta \pmod{N}$.*

Proof. If $\pi(s'\,;\ t',\ R',\ \theta') = \pi(s\,;\ t,\ R,\ \theta)$, then (see Theorem 2, (3)) $t' \equiv t \pmod{n}$, and

$$t'x + s'R'\sum_{i=1}^{x-1}(x-i)\theta'^{i-1} \equiv tx + sR\sum_{i=1}^{x-1}(x-i)\theta^{i-1} \pmod{n}, \quad \text{for } x \geqslant 2\,;$$

i.e.

$$s'R'\sum_{i=1}^{x-1}(x-i)\theta'^{i-1} \equiv sR\sum_{i=1}^{x-1}(x-i)\theta^{i-1} \pmod{n} \quad (x \geqslant 2). \qquad \ldots\ldots\ldots\ldots\ldots\ldots(11)$$

For $x = 2$, we have

$$s'R' \equiv sR \pmod{n}, \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(12)$$

and therefore $(s'R',\ s'N') = (sR,\ sN)$; but since $(R,\ N) = 1$ and $(R',\ N') = 1$, it follows that $s' = s$, and hence, by (12), $R' \equiv R \pmod{N}$. Moreover, by using (12) and (11), with $x = 3$, we deduce that $\theta' \equiv \theta \pmod{N}$. This confirms the conditions in the lemma. The converse of the

https://doi.org/10.1017/S2040618500033657 Published online by Cambridge University Press

lemma is trivial and the proof is therefore omitted.

The preceding two lemmas combine together to prove

THEOREM 3. *No two permutations of the same class can be identical.*

We are now in a position to distinguish permutations of different classes. We prove the following

THEOREM 4. $\pi(s'\ ;\ t, R, \theta) = \pi(s\ ;\ \lambda, \omega)$ *if and only if*

$$s' = ks, \text{ where } k = (\omega - 1, N),\ t \equiv 1 + \lambda s \pmod{n}, \quad \ldots\ldots (13)$$

$$R \equiv \frac{\lambda(\omega - 1)}{k} \pmod{N'}, \quad \theta \equiv \omega \pmod{N'}, \quad N' = \frac{n}{s'} = \frac{N}{k}, \quad \ldots\ldots (14)$$

$$u + \frac{\lambda b}{s}\left\{ht^{h-1} - \frac{t^h - 1}{t - 1}\right\} \text{ is prime to } N', \quad \ldots\ldots (15)$$

$$uk(1 + \lambda s) - \lambda h(1 + uks) \equiv 0 \pmod{N'}, \quad \ldots\ldots (16)$$

where h is the order of t modulo s', u is defined modulo N' by $t^h \equiv 1 + us' \pmod{n}$ and

$$b \equiv \frac{\omega - 1}{k} \sum_{i=1}^{s-1} (s - i)\omega^{i-1} \pmod{N'}.$$

Proof. Suppose that $\pi(s'\ ;\ t, R, \theta) = \pi(s\ ;\ \lambda, \omega)$; then (see Theorem 1, (1) and Theorem 2, (3))

$$t \equiv 1 + \lambda s \pmod{n} \quad \ldots\ldots (17)$$

and
$$tx + s'R \sum_{i=1}^{x-1} (x - i)\theta^{i-1} \equiv x + s\lambda(1 + \omega + \ldots + \omega^{x-1}) \pmod{n}, \text{ for } x \geqslant 2. \quad \ldots\ldots (18)$$

If we put $t \equiv 1 + \lambda s \pmod{n}$, (18) takes the form

$$s'R \sum_{i=1}^{x-1} (x - i)\theta^{i-1} \equiv s\lambda(\omega - 1) \sum_{i=1}^{x-1} (x - i)\omega^{i-1} \pmod{n}, \text{ for } x \geqslant 2. \quad \ldots\ldots (19)$$

For $x = 2$, we have

$$s'R \equiv s\lambda(\omega - 1) \pmod{n}, \quad \ldots\ldots (20)$$

which gives (since $(R, N') = 1$ and $(\lambda, N) = 1$)

$$s' = s(\omega - 1, N) = ks, \quad N' = \frac{N}{(\omega - 1, N)} = \frac{N}{k}, \quad \ldots\ldots (21)$$

and accordingly

$$R \equiv \frac{\lambda(\omega - 1)}{(\omega - 1, N)} \equiv \frac{\lambda(\omega - 1)}{k} \pmod{N'}. \quad \ldots\ldots (22)$$

Furthermore, if we put $x = 3$ in (19) and use (20), we find that

$$(\omega - 1)(\theta - \omega) \equiv 0 \pmod{N},$$

and therefore
$$\theta \equiv \omega \pmod{N'}. \quad \ldots\ldots (23)$$

Relations (17), (21), (22) and (23) show the necessity of conditions (13) and (14). We now show that (15) and (16) are necessary for the existence of $\pi(s'\ ;\ t, R, \theta)$, when s', t, R and

https://doi.org/10.1017/S2040618500033657 Published online by Cambridge University Press

θ are given by (13) and (14). In fact, with the choice of s', t, R, θ according to (13) and (14), conditions (5) and (8) (with s' in place of s and N' in place of N) are secured. For, since

$$N' = \frac{N}{(\omega - 1, N)},$$

we have by Theorem 1 (2),

$$1 + \omega + \ldots + \omega^{s-1} \equiv 0 \pmod{N'}.$$

Furthermore, since $\theta \equiv \omega \pmod{N'}$ and $s' = ks$, we have

$$1 + \theta + \ldots + \theta^{s'-1} \equiv (1 + \omega + \ldots + \omega^{s-1})(1 + \omega^s + \ldots + \omega^{(k-1)s}) \equiv 0 \pmod{N'};$$

this confirms condition (5) of Theorem 2.

Again, since $\theta \equiv \omega \pmod{N'}$ and $t \equiv 1 + s\lambda \pmod{n}$, we have

$$\theta^{rt^i} - \theta^r \equiv \omega^{rt^i} - \omega^r \equiv \omega^{r(1+s\lambda)^i} - \omega^r \pmod{N'}$$
$$\equiv 0 \pmod{N'},$$

because $\omega^s \equiv 1 \pmod{N}$ and $N = kN'$; this confirms condition (8) of Theorem 2.

Next, we proceed to show that conditions (6) and (7) reduce respectively to conditions (15) and (16) of the theorem. For, since $R \equiv \lambda(\omega - 1)/k \pmod{N'}$ and $\theta \equiv \omega \pmod{N'}$, then (see Theorem 2, (4))

$$\psi(x) \equiv \frac{\lambda(\omega - 1)}{k} \sum_{i=1}^{x-1} (x - i)\omega^{i-1} \pmod{N'},$$

and therefore
$$k\psi(x) \equiv \lambda(1 + \omega + \ldots + \omega^{x-1} - x) \pmod{N}.$$

For $x = 1 + ys$, we have

$$k\psi(1 + ys) \equiv \lambda\{(1 + \omega + \ldots + \omega^{s-1})(1 + \omega^s + \ldots + \omega^{(y-1)s}) + \omega^{ys} - 1 - ys\} \pmod{N}$$
$$\equiv \lambda y(1 + \omega + \ldots + \omega^{s-1} - s) \pmod{N}$$
$$\equiv \lambda y(\omega - 1) \sum_{i=1}^{s-1} (s - i)\omega^{i-1} \pmod{N}.$$

If we divide both sides by k and put $b \equiv \frac{\omega - 1}{k} \sum_{i=1}^{s-1} (s - i)\omega^{i-1} \pmod{N'}$, we find that

$$\psi(1 + ys) \equiv \lambda by \pmod{N'}. \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (23)$$

In a similar way, we can also show that

$$\psi(2 + ys) \equiv \lambda by + \frac{\lambda(\omega - 1)}{k} \pmod{N'}. \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (24)$$

We turn now to conditions (6) and (7) of Theorem 2. Condition (7) requires that

$$u + \sum_{i=0}^{h-1} t^{h-i-1}\psi(t^i)$$

is prime to N'; but since $t \equiv 1 + \lambda s \pmod{n}$, then, by using (23), it follows that

$$\psi(t^i) \equiv \lambda b \frac{t^i - 1}{s} \pmod{N'},$$

and condition (6) is then secured if

$$u + \frac{\lambda b}{s}\left\{ht^{h-1} - \frac{t^h - 1}{t - 1}\right\}$$

https://doi.org/10.1017/S2040618500033657 Published online by Cambridge University Press

is prime to N'. Moreover, condition (7) requires that

$$u(\theta-1)\equiv\sum_{i=0}^{h-1}t^{h-i-1}\{\psi(2t^i)-(\theta+1)\psi(t^i)\}\pmod{N'};$$

but, since $\theta\equiv\omega \pmod{N'}$, $\psi(1)\equiv 0 \pmod{N'}$ and $\psi(2)\equiv R\equiv\lambda(\omega-1)/k \pmod{N'}$, then by using (23) and (24), the above condition reduces to

$$u(\omega-1)\equiv t^{h-1}\frac{\lambda(\omega-1)}{k}+\sum_{i=1}^{h-1}t^{h-i-1}\left\{2\lambda b\frac{t^i-1}{s}+\frac{\lambda(\omega-1)}{k}-(\omega+1)\lambda b\frac{t^i-1}{s}\right\}\pmod{N'},$$

i.e. to

$$u(\omega-1)\equiv\frac{\lambda(\omega-1)}{k}\frac{t^h-1}{t-1}+\frac{\lambda b(1-\omega)}{s}\left\{ht^{h-1}-\frac{t^h-1}{t-1}\right\}\pmod{N'};\qquad\ldots\ldots\ldots(25)$$

moreover,
$$b(1-\omega)\equiv-(\omega-1)\frac{\omega-1}{k}\sum_{i=1}^{s-1}(s-i)\omega^{i-1}\pmod{N'}$$

$$\equiv s\frac{\omega-1}{k}\pmod{N'},$$

since $\omega^s-1\equiv 0 \pmod{kN'}$, and so (25) takes the form

$$u(\omega-1)\equiv\frac{\lambda(\omega-1)}{k}ht^{h-1}\pmod{N'},$$

or simply
$$uk\equiv\lambda ht^{h-1}\pmod{N'}.$$

If we multiply both sides by $t\equiv 1+\lambda s \pmod{n}$ (note that such an operation has no effect on the condition under consideration because t is prime to n and therefore to N') and put $t^h\equiv 1+uks \pmod{n}$, the above condition then takes the form

$$uk(1+\lambda s)\equiv\lambda h(1+uks)\pmod{N'},$$

which confirms (16). Thus we have shown the necessity of all the conditions in the theorem.

For the converse, it has been shown that (15) and (16) are sufficient for the existence of $\pi(s';\ t, R, \theta)$ when s', t, R and θ are given by (13) and (14). Then it remains to show that, in virtue of (13) and (14), $\pi(s';\ t, R, \theta)=\pi(s;\ \lambda, \omega)$.

Denoting $\pi(s;\ \lambda, \omega)$ by π and $\pi(s';\ t, R, \theta)$ by π', and using (13) and (14), we find that

$$\pi' 1\equiv t\equiv 1+\lambda s\pmod{n},\qquad\ldots\ldots\ldots(26)$$

and, for $x\geqslant 2$,
$$\pi' x\equiv tx+s'R\sum_{i=1}^{x-1}(x-i)\theta^{i-1}\pmod{n}$$

$$\equiv x(1+\lambda s)+s\lambda(\omega-1)\sum_{i=1}^{x-1}(x-i)\omega^{i-1}\pmod{n};$$

i.e.
$$\pi' x\equiv x+s\lambda(1+\omega+\ldots+\omega^{x-1})\pmod{n},\quad\text{for } x\geqslant 2.\qquad\ldots\ldots\ldots(27)$$

(26) and (27) combine together to show that $\pi'=\pi$, *i.e.* $\pi(s';\ t, R, \theta)=\pi(s;\ \lambda, \omega)$. This completes the proof of the theorem.

The above theorem may be illustrated by the following example.

https://doi.org/10.1017/S2040618500033657 Published online by Cambridge University Press

3. Illustrative example. Let $n=p^4$, where p is an odd prime, and consider the two semi-special permutations (see [2, § 5]) $\pi=\pi(p;\ \lambda,\ 1+\Omega p^2)$ and $\pi'=\pi(p^3;\ t,\ R,\ 1)$ defined on $[p^4]$ by

$$\pi x \equiv x+\lambda p x+\tfrac{1}{2}\lambda\Omega p^3 x(x-1) \pmod{p^4},$$
$$\pi' x \equiv tx+\tfrac{1}{2}Rp^3 x(x-1) \pmod{p^4},$$

where λ, Ω, R and t are all prime to p ; $t\not\equiv 1 \pmod{p^3}$ and t, R are chosen in such a way that $u-\frac{1}{2}Rht^{h-1}$ is prime to p, h being the order of t modulo p^3, and u is defined modulo p by $t^h\equiv 1+up^3 \pmod{p^4}$.

If we take $t\equiv 1+\lambda p \pmod{p^4}$, $R\equiv\lambda\Omega \pmod{p}$, then $h=p^2$ and $u\equiv\lambda \pmod{p}$; in this case $u-\frac{1}{2}Rht^{h-1}\equiv\lambda \pmod{p}$ which is prime to p and $\pi'=\pi$, *i.e.*

$$\pi(p^3\ ;\ 1+\lambda p,\ \lambda\Omega,\ 1)=\pi(p\ ;\ \lambda,\ 1+\Omega p^2).$$

On the other hand the conditions of Theorem 4 can be easily confirmed in this case with $s=p$, $N=p^3$, $\omega\equiv 1+\Omega p^2 \pmod{p^3}$, $s'=p^3$, $N'=p$, $t\equiv 1+\lambda p \pmod{p^4}$, $R\equiv\lambda\Omega \pmod{p}$ and $\theta\equiv 1 \pmod{p}$.

REFERENCES

1. K. R. Yacoub, On semi-special permutations I, *Proc. Glasgow Math. Assoc.*, **3** (1956), 18–35.

2. ——, On semi-special permutations II. Semi-special permutations on $[p^\alpha]$, *Duke Math. J.*, **24** (1957), 455–465.

FACULTY OF SCIENCE
ALEXANDRIA UNIVERSITY
EGYPT