A NOTE ON THE CLASSES OF NON-LINEAR SEMI-SPECIAL PERMUTATIONS

by K. R. YACOUB

(Received 31st March, 1958)

In a recent paper [**1**], the author divided the semi-special permutations on $[n]$ that are not linear into two classes. The first class consists of the semi-special permutations which, for all possible values of s, have s as a principal number and which induce modulo s the identity permutation. The second class consists of all the semi-special permutations, with principal number s, which induce modulo s linear permutations other than the identity, where again s takes all its possible values.

Further, it was shown that no two permutations of the same class (though with different values of the parameter s) can be identical [**1**, Theorem 3]. It was also shown that, under certain conditions, a permutation of the first class may be identical with a permutation of the second class [**1**, Theorem 4]. This fact raised a question of some interest, namely, whether one of the classes is perhaps a subclass of the other. The answer to this question is, in a few cases, affirmative.

However, in some cases there exists one and only one class of such permutations. For example, if $n = 2p$, where p is an odd prime, the non-linear semi-special permutations on $[2p]$ are of the form

$$\pi(2x) = 2x, \quad \pi(2x+1) \equiv 2x+1+2\lambda \pmod{2p},$$

where λ is prime to p [**2**, Theorem 4.1]. It is evident that, in this case, the permutations just described constitute only one class, namely, the first class, and the second class is in fact empty.

Furthermore, if $n = p^2$, where p is an odd prime, the non-linear semi-special permutations on $[p^2]$ are of the form

$$\pi x \equiv tx + p\mu x(x-1) \pmod{p^2},$$

with $t \not\equiv 1 \pmod{p}$, where t and μ are both prime to p and are chosen such that $u - \mu h t^{h-1}$ is also prime to p, h being the order of t modulo p, and u defined modulo p by $t^h \equiv 1 + up \pmod{p^2}$ [**2**, Theorem 4.2]. These permutations constitute again one class, namely, the second class. In this case, the first class is empty.

Nevertheless, if $n = p^3$ or p^4, where p is an odd prime, the two classes do exist, but the first class is actually a subclass of the second [**3**, Theorems 8 and 9]. It is, however, interesting to see whether this fact remains true for higher powers of p. This is the main object of this note.

In the following paragraph, we collect the notations and results we require here.

1. Notations and Miscellaneous Results.

In an earlier paper [**2**], it was shown that if π be a non-linear semi-special permutation on $[n]$ with principal number s, then it is either of the form

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

or of the form

https://doi.org/10.1017/S2040618500033761 Published online by Cambridge University Press

$$\pi 1 = t, \quad \pi x \equiv tx + sR\sum_{i=1}^{x-1}(x-i)\theta^{i-1} \pmod{n} \quad (x \geqslant 2), \quad \text{.....................(2)}$$

where $t \not\equiv 1 \pmod{s}$, according as the permutation induced by π modulo s is the identity permutation or is not. The parameters λ, ω, t, R and θ are to be chosen in the proper way [**2**, Theorems 3.1 and 3.10].

We remark that, when n is given, the permutation π defined by (1) depends on three parameters, namely s, λ and ω, and is denoted by $\pi(s\,;\ \lambda, \omega)$. Furthermore, the permutation π defined by (2) depends on four parameters, namely s, t, R and θ, and may therefore be denoted by $\pi(s\,;\ t, R, \theta)$. It should be noted that the parameters s and t are to be determined modulo n, while the parameters λ, ω, R and θ are to be determined modulo N, where $N = n/s$.

THEOREM 1. *With the above notation,* $\pi(s\,;\ \lambda, \omega) = \pi(s'\,;\ t, R, \theta)$ *if and only if*

$$s' = ks, \ t \equiv 1 + \lambda s \pmod{n}\,; \quad \text{.....................................(3)}$$

$$R \equiv \frac{\lambda(\omega-1)}{k}, \quad \theta \equiv \omega \pmod{N'} \quad \left[k = (\omega-1, N), N = \frac{n}{s}, \ N' = \frac{n}{s'} = \frac{N}{k}\right]; \quad \text{......(4)}$$

$$u + \frac{\lambda b}{s}\left\{ht^{h-1} - \frac{t^h-1}{t-1}\right\} \text{ is prime to } N'\,; \quad \text{..............................(5)}$$

$$uk(1+\lambda s) - \lambda h(1+uks) \equiv 0 \pmod{N'}, \quad \text{..............................(6)}$$

where h is the order of t modulo s' and u is defined modulo N' by $t^h \equiv 1 + us' \pmod{n}$, *and where* [**1**, Theorem 4]

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

Note. It should be pointed out that conditions (5) and (6) are in fact the necessary and sufficient conditions for the existence of $\pi(s'\,;\ t, R, \theta)$ when s', t, R and θ are given by (3) and (4).

THEOREM 2(*a*). *Let p be an odd prime, and $\alpha > 2$, and let λ, t, R, Ω and Θ all be prime to p. Then the non-linear semi-special permutations on* $[p^\alpha]$, *with principal number* p^β, *are* (i)

$$\pi x \equiv x + p^\beta\lambda\,(1+\omega+\ldots+\omega^{x-1}) \pmod{p^\alpha},$$

for $\beta < \alpha - 1$, *where* $\omega \equiv 1 + \Omega p^\gamma \pmod{p^{\alpha-\beta}}$, *with* $\gamma = 1, \ldots, \alpha-\beta-1$ *if* $2\beta \geqslant \alpha$, *and* $\gamma = \alpha - 2\beta, \ldots, \alpha-\beta-1$ *if* $2\beta < \alpha$, *and* (ii)

$$\pi 1 = t, \quad \pi x \equiv tx + p^\beta R\sum_{i=1}^{x-1}(x-i)\theta^{i-1} \pmod{p^\alpha} \quad (x \geqslant 2),$$

for $\beta \geqslant \frac{1}{2}\alpha$, *where* $t \not\equiv 1 \pmod{p^\beta}$ *and* $\theta \equiv 1 + \Theta p^\delta \pmod{p^{\alpha-\beta}}$ *with* $\delta = 1, \ldots, \alpha-\beta$, *and where t, R and Θ are to be chosen properly* [**3**, Theorems 5 and 6].

Using the previous notation, we may write the above theorem as

THEOREM 2(*b*). *Let* $n = p^\alpha$, *where p is an odd prime and* $\alpha > 2$, *and let λ, t, R, Ω* and *Θ be chosen as in Theorem* 2(*a*). *Then the non-linear semi-special permutations on* $[p^\alpha]$ *are* (i)

$$\pi(p^\beta;\ \lambda, 1+\Omega p^\gamma),$$

for $\beta < \alpha - 1$, *with* $\gamma = 1, \ldots, \alpha \quad \beta - 1$ *if* $2\beta \geqslant \alpha$, *and* $\gamma = \alpha - 2\beta, \ldots, \alpha-\beta-1$ *if* $2\beta < \alpha$, *and* (ii)

$$\pi(p^{\beta^*}\,;\ t, R, 1+\Theta p^\delta),$$

for $\beta^* \geqslant \frac{1}{2}\alpha$, *with* $\delta = 1, \ldots, \alpha - \beta$.

https://doi.org/10.1017/S2040618500033761 Published online by Cambridge University Press

2. The Main Results.

We start by proving the following

THEOREM 3. *Let the notation be as in Theorem 2(b), and let* $\beta<\alpha-1$. *Then*

$$\pi(p^\beta;\ \lambda,\ 1+\Omega p^\gamma) = \pi(p^{\beta^*};\ 1+\lambda p^\beta, \lambda\Omega, 1+\Omega p^\gamma),$$

where $\beta^*=\beta+\gamma$.

Proof. Suppose that

$$\pi(p^\beta;\ \lambda,\ 1+\Omega p^\gamma) = \pi(s;\ t, R, \theta);$$

then, by Theorem 1, we have

$$s = (\Omega p^\gamma, p^{\alpha-\beta}) \times p^\beta = p^{\beta+\gamma} = p^{\beta^*},$$

because Ω is prime to p,

$$t \equiv 1+\lambda p^\beta \pmod{p^\alpha},$$

and

$$R \equiv \lambda\Omega, \quad \theta \equiv 1+\Omega p^\gamma \pmod{p^{\alpha-\beta^*}}.$$

It remains to show that with these values of s, t, R and θ, conditions (5) and (6) are satisfied identically. Here h is the order of t modulo s, where $t\equiv 1+\lambda p^\beta \pmod{p^\alpha}$ and $s=p^{\beta^*}$; also u is defined modulo $p^{\alpha-\beta^*}$ by $t^h=1+up^{\beta^*} \pmod{p^\alpha}$.

Now, since $t\equiv 1+\lambda p^\beta \pmod{p^\alpha}$ and λ is prime to p, it follows that $h=p^\gamma$, and then $u\equiv\lambda(1+Up^\beta) \pmod{p^{\alpha-\beta^*}}$ for some integer U. Also

$$ht^{h-1}-\frac{t^h-1}{t-1} \equiv p^\gamma(1+\lambda p^\beta)^{p^\gamma-1} - \sum_{i=1}^{p^\gamma}\binom{p^\gamma}{i}(\lambda p^\beta)^{i-1} \pmod{p^\alpha}$$

$$\equiv p^{\beta+\gamma}T \pmod{p^\alpha},$$

for some integer T. Condition (5) then requires that

$$\lambda(1+Up^\beta)+\lambda bp^\gamma T$$

is prime to p, which is already secured since λ is prime to p [see Theorems 2(b) and 2(a)]. Moreover, condition (6) reduces to

$$\lambda(1+Up^\beta)\, p^\gamma\, (1+\lambda p^\beta) - \lambda p^\gamma\, \{1+\lambda(1+Up^\beta)\, p^{\gamma+\beta}\} \equiv 0 \pmod{p^{\alpha-\beta^*}},$$

i.e. to

$$\lambda p^{\beta^*}\{U+\lambda+U\lambda p^\beta-\lambda\,(1+Up^\beta)\,p^\gamma\} \equiv 0 \pmod{p^{\alpha-\beta^*}}. \quad\ldots\ldots\ldots\ldots(7)$$

Condition (7) is secured if $2\beta^*\geqslant\alpha$.

We now show that $2\beta^*\geqslant\alpha$. For if $\beta\geqslant\frac{1}{2}\alpha$, we have $2\beta^*=2\beta+2\gamma>2\beta>\alpha$; also when $\beta<\frac{1}{2}\alpha$, γ takes one of the values $\alpha-2\beta, \ldots, \alpha-\beta-1$ and thus $2\beta^*>\alpha$. Hence condition (6) is, for all $\beta<\alpha-1$, secured and the theorem is proved.

Theorem 3 leads at once to the following theorem.

THEOREM 4. *Let* p *be an odd prime and* $\alpha>2$. *Then the two classes of non-linear semi-special permutations on* $[p^\alpha]$ *are both non-empty. Moreover the first class is always a subclass of the second.*

When $\alpha=2$, the first class is empty and the second part of the theorem is trivial.

https://doi.org/10.1017/S2040618500033761 Published online by Cambridge University Press

REFERENCES

1. K. R. Yacoub, A note on semi-special permutations, *Proc. Glasgow Math. Assoc.*, **3** (1958), 164–169.

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

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

FACULTY OF SCIENCE
ALEXANDRIA UNIVERSITY
EGYPT

https://doi.org/10.1017/S2040618500033761 Published online by Cambridge University Press