On Perfect 3– and 4–Shift N–Designs

Ulrich Tamm[1], *Member, IEEE*

Abstract. Necessary and sufficient conditions for the existence of perfect 3– and 4–shift N–designs are presented. From these perfect shift designs perfect run length limited codes capable of correcting single peak shifts of size 3 and 4 can be obtained. The results extend to the more general class of perfect $\mathcal{S}$– shift N–designs for sets $\mathcal{S} = \{1, a, \dots, a^r, b, \dots, b^s\}$.

Index terms. Peak-shift correction, perfect shift designs

1)
Ulrich Tamm
Dept. of Mathematics
University of Bielefeld
P. O. Box 100131
33501 Bielefeld
Germany
E–mail tamm@mathematik.uni-bielefeld.de

I. Introduction

In [1] Levenshtein and Vinck investigated perfect run–length–limited codes which are capable of correcting single peak shifts. As a basic combinatorial tool for the construction of such codes they introduced the concept of a *t–shift N–design*, which is defined to be an N–elementary subset $\mathcal{H} = \{h_1, \dots h_N\}$ of a finite additive Abelian group $\mathcal{G}$, with the property that for any $\sigma = 1, \dots t$ and any $i = 1, \dots, N$ all $2Nt$ elements $\pm\sigma \cdot h_i$ are different and not equal to zero. Such a design is said to be *perfect* if $|\mathcal{G}| = 2tN + 1$, i. e., for every element $g \in \mathcal{G}$ there are exactly one $h_i \in \mathcal{H}$ and $\sigma \in \{1, \dots, t\}$ such that $g = \sigma \cdot h_i$ or $g = -\sigma \cdot h_i$.
Vinck and Levenshtein [1] also gave explicit constructions of perfect t–shift designs for the special values $t = 1, 2$ and for the case $t = \frac{p-1}{2}$, $N = (p^\nu - 1)/(p-1)$, where p is a prime number.

In this note we shall investigate perfect t–shift N–designs in Z_{2tN+1}, the ring of integers modulo $2tN + 1$, for the parameters $t = 3$ and $t = 4$. In order to do so, we shall first introduce a more general shift design concept.
We call a subset $\mathcal{H} = \{h_1, \dots h_N\}$ of a finite (not necessarily additive) Abelian group $\mathcal{G}$ an *$\mathcal{S}$–shift N–design* if for any $\sigma \in \mathcal{S}$ and any $i = 1, \dots, N$ all $|\mathcal{S}| \cdot N$ elements $\sigma \cdot h_i$ are different and not equal to zero. Sometimes we shall omit the parameters $\mathcal{S}$ or N and only speak of a shift design or an $\mathcal{S}$–shift design.
So, the set $\mathcal{S}$ is no longer considered to be an interval. The t–shift designs in an additive Abelian group $\mathcal{G}'$ arise as a special case by considering $\mathcal{S}$–shift designs in the group $\mathcal{G} = \mathcal{G}' \backslash \{1, -1\}$, with the special choice $\mathcal{S} = \{1, \dots, t\}$ (since only one of the elements h and $-h$ can be contained in a design $\mathcal{H}$, we can identify them by considering the group $\mathcal{G}'$ modulo the units $\{1, -1\}$).
Perfectness is defined as before, i. e., every element $g \in \mathcal{G}$ has a unique representation $g = \sigma \cdot h$ for some $\sigma \in \mathcal{S}$ and $h \in \mathcal{H}$.
Observe that every perfect $\mathcal{S}$–shift N–design $\mathcal{H}$ in a group $\mathcal{G} = \mathcal{G}' \backslash \{1, -1\}$ yields a perfect $\mathcal{S}$–shift N–design $\mathcal{H}' = \mathcal{H} \cup (-\mathcal{H})$ in $\mathcal{G}'$.

In order to study 3– and 4– shift N–designs, we shall first investigate $\mathcal{S}$–shift N–designs for sets $\mathcal{S}$ of the form

$$\mathcal{S} = \{1, a, a^2, \dots, a^r, b, b^2, \dots b^s\}, \tag{1}$$

where $r > 1$ and $s > 1$ are nonnegative integers smaller than the orders of a and b in $\mathcal{G}$, respectively, which we shall denote by $\mathrm{ord}(a)$ and $\mathrm{ord}(b)$.
Observe that with $a = 2$ and $b = 3$ we obtain $\mathcal{S} = \{1, 2, 3\}$ for $r = s = 1$ and $\mathcal{S} = \{1, 2, 3, 4\}$ for $r = 2, s = 1$. Hence the 3–shift and 4–shift N–designs we want to study in this paper occur for a special choice of the parameters.
In order to characterize the structure of a perfect $\mathcal{S}$–shift N–designs with $\mathcal{S}$ defined as in (1), we first need some further notation. As usual, we denote by

$$< a, b >= \{a^i \cdot b^j, i = 1, \dots \mathrm{ord}(a), j = 1, \dots \mathrm{ord}(b)\} \tag{2}$$

the subgroup of $\mathcal{G}$ generated by the elements a and b. Furthermore let

$$\mathcal{F} = \{a^i \cdot b^j, i - j \equiv 0 \bmod (r + s + 1)\}. \tag{3}$$

Observe that $\mathcal{F}$ is the subgroup in $\mathcal{G}$ generated by the elements a^{r+s+1}, b^{r+s+1} and ab. It can be shown that a perfect $\mathcal{S}$–shift N–design in the group $\mathcal{G}$ exists exactly if for each element $f \in \mathcal{F}$ all possible representations $f = a^i \cdot b^j$ as a product of powers of a and b are such that $i - j \equiv 0 \bmod (r + s + 1)$. Necessary and sufficient conditions are given in the following theorem.

Theorem 1: Let $\mathcal{S} = \{1, a, a^2, \dots, a^r, b, b^2, \dots b^s\}$ be defined as in (1). A perfect $\mathcal{S}$–shift N–design in $\mathcal{G}$ is of the form

$$\mathcal{H} = \mathcal{F} \cup x_1 \cdot \mathcal{F} \cup \dots \cup x_{\rho-1} \cdot \mathcal{F}, \tag{4}$$

where ρ is the number of conjugacy classes of the subgroup $< a, b >$ and the $x_i, i = 1, \ldots, \rho - 1$ are representatives of each of these conjugacy classes, and where

$$\mathrm{ord}(a) \text{ and } \mathrm{ord}(b) \text{ are divisible by } r + s + 1. \tag{5}$$

Further, if $b^{l_1} = a^{l_2}$ for some $l_1 \in \{1, \ldots, \mathrm{ord}(a)\}, l_2 \in \{1, \ldots, \mathrm{ord}(b)\}$, then

$$l_1 + l_2 \equiv 0 \bmod (r + s + 1) \tag{6}$$

Theorem 1 will be proved in Section II. As mentioned before, the group we are interested in, is $\mathcal{G} = Z_n^* \backslash \{1, -1\}$, the multiplicative group of residues relatively prime to the positive integer $n = 2 \cdot \mathcal{S} \cdot N + 1$, where (following the example of a perfect 2–shift N–design in [1]) the elements g and $-g$ are identified for all $g \in G$.

In principle, the perfect $\mathcal{S}$–shift N–designs for sets of the form (1) are completely characterized by Theorem 1. However, in order to find such perfect shift designs, several conditions imposed on the orbit of the elements a and b by (5) and (6) have to be verified.

This will be done in Section III for sets of the form $\mathcal{S} = \{1, a, b\}$ and $\mathcal{S} = \{1, a, a^2 b\}$, from which the perfect 3– and 4–shift N–designs (as defined by Levenshtein and Vinck in [1]) in Z_{6N+1} and Z_{8N+1}, respectively, can be obtained by the special choice of the parameters $a = 2$ and $b = 3$.

II. Perfect $\{1, a, \ldots, a^r, b, \ldots b^s\}$–shift N–designs

We saw already that $\mathcal{F}$ is generated by the elements a^{r+s+1}, b^{r+s+1} and ab in $\mathcal{G}$. The next lemma shows that with $x \in \mathcal{H}$ these three elements multiplied by x necessarily are also contained in $\mathcal{H}$.

Lemma 1: In a perfect $\mathcal{S}$–shift N–design $\mathcal{H}$, where $\mathcal{S}$ is of the form (1), with every element $x \in \mathcal{H}$, also $(ab)x \in \mathcal{H}$ and $a^{r+s+1}x$ and $b^{r+s+1}x$ must be the next powers of a and b, respectively, which multiplied by x are contained in $\mathcal{H}$.

Proof: Let $x \in \mathcal{H}$ be an element of a perfect $\mathcal{S}$–shift N–design $\mathcal{H}$. Then $(ab)x$ must also be contained in $\mathcal{H}$. If this would not be the case, then $(ab)x = a^k y$ for some $k \in \{1, \ldots, r\}$ and $y \in \mathcal{H}$ or $(ab)x = b^l y'$ for some $l \in \{1, \ldots, s\}$ and $y' \in \mathcal{H}$. If $(ab)x = a^k y$ then $x' = bx = a^{k-1}y$ and x' would have two different representations $\sigma h, \sigma' h'$ with $\sigma, \sigma' \in \mathcal{S}$ and $h, h' \in \mathcal{H}$, which contradicts the definition of a shift design. Analogously, if $(ab)x = a^k y$ then $x' = bx = a^{k-1}y$ would have two different representations, which is not possible.

Now let k^* be the minimum power k such that $a^k x \in \mathcal{H}$ for some $x \in \mathcal{H}$. We have to show that $k^* = r + s + 1$.

First observe that obviously $k^* \geq r + 1$, since otherwise $x' = a^{k^*} (= 1 \cdot x')$ would occur in two different ways as product of elements of $\mathcal{S}$ and $\mathcal{H}$.

In order to see that $k^* \notin \{r + 1, \ldots, r + s\}$, we shall prove by induction the stronger statement

$$\text{If } x \in \mathcal{H} \text{ then for all } i = 1, \ldots s \text{ it is } a^{r+i}x = b^{s+1-i}y_i \text{ for some } y_i \in \mathcal{H} \tag{7}$$

The statement (7) holds for $i = 1$, since $a^{r+1}x = b^j y$ for some $y \in \mathcal{H}$ and $j \in \{0, \ldots, s - 1\}$ is not possible. Otherwise, $a^{r+1}bx = a^r(abx) = b^{j+1}y$ could be written in two different ways as product of members of the shift design (abx and y) and elements of $\mathcal{S}$ (a^r and b^{j+1}).

So assume that (7) holds for $1 \leq i \leq s - 1$. Then $a^{r+i+1} = b^j y$ for some $y \in \mathcal{H}$ and $j \in \{0, \ldots, s - i - 1\}$ is not possible, since otherwise $a^{r+i+1}b^{i+1}x = a^r((ab)^{i+1}x) = b^{j+i+1}y$ with the same argumentation as in the induction beginning.

Also $a^{r+i+1}x = b^j y$ for some $y \in \mathcal{H}$ and $j \in \{s - i + 1, \ldots, s\}$ cannot occur, since in this case by induction $a^{r+i}x = b^{s+1-i}y''$ for some $y'' \in \mathcal{H}$ and hence $a^{r+i+1}b^{-(s+1-i)} = ay'' = b^{j-(s+1-i)}y$ would have two different representations as a product of members of $\mathcal{H}$. Hence $a^{r+i+1}x$ can only occur as the product b^{s-i} in a perfect shift design and (7) is proved.

Using the last argument of the induction step with $i = s$, it is also clear that $a^{r+s+1}x$ must be in $\mathcal{H}$ if $x \in \mathcal{H}$.
Analogously, it can be shown that $r+s+1$ is also the minimum power l^* such that $b^{l^*}x \in \mathcal{H}$ when $x \in \mathcal{H}$ (obviously $l^* > s$ and $l^* \notin \{s+1, \ldots, s+r\}$ by an argument as (7)).

PROOF OF THEOREM 1:

First we shall demonstrate that a set $\mathcal{H}$ with the properties (4), (5), and (6) from Theorem 1 forms a perfect shift design. It suffices to show that every element $z = a^i b^j$ of the subgroup $< a, b >$ generated by the elements a and b can uniquely be obtained from one element $a^{i'}b^{j'}, i' - j' \equiv 0 \bmod (r+s+1)$ in $\mathcal{F}$ by multiplication with a power of a or b from the set $\mathcal{S} = \{1, a, a^2, \ldots a^r, b, b^2, \ldots b^s\}$.
To see this let $z = a^i b^j$ with $i - j \equiv k \bmod (r+s+1)$. If $k = 0$, then z must be contained in $\mathcal{H}$, since $a^l z, l = 1, \ldots, r$ or $b^l z, l = 1, \ldots, s$ are not members of $\mathcal{H}$. If $k \in \{1, \ldots, r\}$, then $z = a^k h = a^k(a^{i-k}b^j)$ is the only possibility to write z as a product of an element (namely a^k) from $\mathcal{S}$ and a member h of $\mathcal{H}$. Finally, if $k \in \{r+1, \ldots, r+s\}$, then $z = b^k h' = b^k(a^i b^{j-k})$ is the unique way of representing z as product of an element (b^k) of $\mathcal{S}$ and one (h') of $\mathcal{H}$.

In order to show that a perfect $\mathcal{S}$–shift design $\mathcal{H}$ must have a group structure as in (4), assume w. l. o. g. that the neutral element $1 \in \mathcal{H}$. Lemma 1 then implies that all powers of a^{r+s+1}, b^{r+s+1} and ab and all combinations of them, i. e., all elements of the form

$$h = (a^{r+s+1})^{k_1}(b^{r+s+1})^{k_2}(ab)^{k_3} = a^{(r+s+1)\cdot k_1 + k_3} b^{(r+s+1)\cdot k_2 + k_3} \tag{8}$$

must be contained in $\mathcal{H}$, which just yields that

$$h = a^i \cdot b^j \text{ for some } i - j \equiv 0 \bmod r+s+1 \tag{9}$$

It is also clear that every element of this form (9) can occur as a combination (8). So all elements of $\mathcal{F}$ as defined under (3) must be contained in $\mathcal{H}$
Further observe that an element of the form $a^i b^j$ with $i - j$ not divisible by $r+s+1$ cannot be contained in a perfect design $\mathcal{H}$ in the subgroup $< a, b >$, since in this case the unique representability would be violated (see above).
Since the elements of a proper conjugacy class $\mathcal{N}$ in $\mathcal{G}$ of $< a, b >$ cannot be obtained from elements of $< a, b >$ by multiplication with powers of a or b, for every such conjugacy class $\mathcal{N}$ we can choose a representative $x_{\mathcal{N}}$ and the elements $x_{\mathcal{N}} \cdot \mathcal{F}$ can be included in the perfect shift design in order to assure that every element from $\mathcal{N}$ can be uniquely written as a product $\sigma \cdot h, \sigma \in \mathcal{S}, h \in \mathcal{H}$.

The conditions (5) and (6) are necessary conditions on the orbits of a and b that must be fulfilled if a perfect shift design should exist in $\mathcal{G}$.
It is easy to verify that the elements a and b each must have an order divisible by $r+s+1$ in order to assure the existence of a perfect $\mathcal{S}$–shift design $\mathcal{H}$ in $\mathcal{G}$. Assume that this would not be the case, e. g.,

$$\text{ord}(a) = k_1 \cdot (r+s+1) + k_2, 0 < k_2 < r+s+1.$$

By Lemma 1 with $x \in \mathcal{H}$ all elements $(a^{r+s+1})^k x$ must also be contained in the perfect shift design $\mathcal{H}$. However, for $k = k_1 + 1$ this yields

$$\mathcal{H} \ni (a^{r+s+1})^{k_1+1}x = a^{(r+s+1)k_1 + k_2 + ((r+s+1) - k_2)}x = a^{r+s+1-k_2}x$$

which is not possible by Lemma 1.
Further, from Lemma 1 we can conclude that with $x \in \mathcal{H}$ also $(ab)^{l_1}x$ and $(ab)^{l_2}x$ for all l_1 and l_2 are contained in a perfect $\mathcal{S}$–shift design $\mathcal{H}$. Now if $a^{l_1} = b^{l_2}$ then $(ab)^{l_1} = a^{l_1}b^{l_1} = b^{l_1+l_2}$,

$(ab)^{l_2} = a^{l_2}b^{l_2} = a^{l_1+l_2}$ and with Lemma 1 and the preceding considerations $l_1 + l_2$ must be divisible by $r + s + 1$.

REMARKS:

1) Observe that the result in Theorem 1 only depends on the number $r + s + 1$ and not on the choice of the set $\mathcal{S}$. So all the sets $\mathcal{S} = \{1, a, \ldots, a^r, b, \ldots, b^s\}$, with the same sum of maximal powers $r + s$ yield the same class of perfect shift designs.

2) Further observe that the group $\mathcal{F}$ fulfilling conditions (5) and (6) also is defined for $i - j \equiv 0 \mod 2$, although this case for our considerations is not of importance since then $r = 0$ or $s = 0$ and one of the parameters a or b will not occur.
However, it can be shown (following the considerations in [1] about 2–shift designs) that a perfect $\{1, a, \ldots a^r\}$ –shift design in a group $\mathcal{G}$ exists exactly if the order of a is divisble by $r + 1$. This is clear, since with $x \in \mathcal{H}$ also $a^{r+1}x$ must be a member of a perfect shift design $\mathcal{H}$ in this case.

3) Finally, observe that the concept of a t–shift design in an additive Abelian group $\mathcal{G}$ has been extended to the concept of an $\mathcal{S}$–shift design in $\mathcal{G}\backslash\{1, -1\}$, where $\mathcal{S}$ can be an arbitrary subset of $\mathcal{G}$. Actually, for this concept the additivity (which is very important for the application in run–length coding) is no longer required. One could also ask the more general question: under which conditions is it possible to represent a group $\mathcal{G}$ as the direct product $\mathcal{S} \times \mathcal{H}$ of two subsets $\mathcal{S}, \mathcal{H} \subset \mathcal{G}$, where each element $g \in \mathcal{G}$ can be written as $g = s \cdot h$ for exactly one $s \in \mathcal{S}$ and $h \in \mathcal{H}$. Observe that the sets $\mathcal{S}$ we considered in this note enforced $\mathcal{H}$ to possess a group structure. It is an interesting question if the same holds for sets of the form $\mathcal{S} = \{1, a, \ldots, a^{r_1}, b, \ldots b^{r_2}, c, \ldots c^{r_3}\}$ This would allow to study 5–shift N–designs for the special choice $\mathcal{S} = \{1, 2, 2^2, 3, 5\}$.

III. PERFECT $\{1, 2, 3\}$– AND $\{1, 2, 3, 4\}$–SHIFT N–DESIGNS

Theorem 1 in principle completely characterizes perfect $\mathcal{S}$– shift designs for sets $\mathcal{S} = \{1, a, \ldots, a^r, b, \ldots b^s\}$. The conditions on the existence of a perfect shift design, however, have to be verified for each group $\mathcal{G}$ individually. Especially, condition (6) requires that many pairs a^ib^j have to be calculated, which can take a lot of time. Sometimes complexity may be reduced by considering the orbit of the element ba^{-1}. If the element a is contained on this orbit, so is $b = a(ba^{-1})$ and it will be shown in the following corollary that the subgroup $\mathcal{F}$ is generated by $(ba^{-1})^3$ in this case.

COROLLARY 1: If a is on the orbit of ba^{-1} in $\mathcal{G}$, i. e., $a = (ba^{-1})^l$ for some l, then

i) $< a, b >= \{(ba^{-1})^k : k = 0, \ldots, \operatorname{ord}(ba^{-1}) - 1\}$ is generated by the element ba^{-1},

ii) For $r = s = 1$, i. e., $r + s + 1 = 3$, $\mathcal{F}$ is generated by $(ba^{-1})^3$, hence

$$\mathcal{F} = \{(ba^{-1})^{3k} : k = 0, \ldots, \frac{1}{3}\operatorname{ord}(ba^{-1}) - 1\},$$

iii) a perfect $\{1, a, b\}$–shift design in $\mathcal{G}$ exists, if

$$l \equiv 1 \mod 3$$

Proof:

i) Observe that $a = (ba^{-1})^l$ and $b = (ba^{-1})^{l+1}$ are contained on the orbit of ba^{-1}. So all products a^ib^j must also be powers of ba^{-1}.

ii) By Theorem 1, a^3, b^3 and ab must be contained in a perfect shift design. By assumption $a^3 = (ba^{-1})^k$ for some k. Now $a^{3+k} = b^k$ and by conditions (5) and (6) k must be divisible by 3. Analogously, $b^3 = (ba^{-1})^k$ for some k, which implies that $b^{k-3} = a^k$ and again by (5) and (6) $k \equiv 0 \mod 3$. Finally, also $ab = (ba^{-1})^k$ for some k, from which follows that $a^{k+1} = b^{k-1}$ which again can only hold if k is divisible by 3.

Finally observe that all powers $(ba^{-1})^{3k} = b^{3k} \cdot a^{\mathrm{ord}(a)-3k}$ are contained in a perfect shift design.

iii) If $l \equiv 0 \bmod 3$, then a would be included in the perfect shift design, and if $l \equiv 2 \bmod 3$, then $b = a(ba^{-1})^{l+1}$ would be included in the perfect shift design. Both possibilities are forbidden by Theorem 1 and hence it must hold $l \equiv 1 \bmod 3$.

With the set $\mathcal{S} = \{1, a, b\}$ the 3–shift designs arise for the special choice of the parameters $a = 2$ and $b = 3$.

Perfect shift designs are much faster to find if the subgroup $\mathcal{F}$ is generated by one element and one might check the orbit of 2, 3, or $3 \cdot 2^{-1}$ by Theorem 1 and Corollary 1.

For prime numbers $p = 6N+1$ besides the trivial design $\{1\}$ in Z_7 the first perfect 3–shift design in Z_p, occurs for $p = 37$, e. g. $\mathcal{H} = \{1, 8, 10, 6, 11, 14\} \subset Z_{37}$. The next perfect 3–shift designs for primes up to 1000 exist in Z_p for $p =$ 139, 163, 181, 241, 313, 337, 349, 379, 409, 421, 541, 571, 607, 631, 751, 859, 877, 919, 937.

If $n = 6N + 1$ is a composite number, then observe that for every proper divisor m of n the multiples of m form a subgroup isomorphic to $Z_{n/m}$. Hence a necessary condition on the number n to assure the existence of a perfect 3–shift design is that in every subgroup Z_m, where m divides n, a perfect 3–shift design must exist. So, in each case n must be the product of prime numbers which are congruent 1 modulo 6.

The remaining $\varphi(n)$ elements in Z_n^* are relatively prime to n. If $\varphi(n) \equiv 0 \pmod 6$ and a and b are relatively prime to n (as it is the case for $a = 2$ and $b = 3$), then Theorem 1 can be applied with $\mathcal{G} = Z_n^* \backslash \{1, -1\}$ This way it can be shown that there exists a perfect 3–shift 8–design in Z_{49}, e.g. $\mathcal{H} = \{1, 15, 20, 6, 8, 22, 13\} \cup \{7\}$. The same design had been obtained in [1] using different methods – observe that $3 = \frac{p-1}{2}$ for $p = 7$.

4–shift N–designs arise from the set $\{1, a, a^2, b\}$ for the special choice of the parameters $a = 2$ and $b = 3$. Again it might be useful to consider the orbit of further elements besides a and b to speed up the computation of an algorithm which finds perfect shift designs. Some results are collected in the subsequent corollary.

Corollary 2: If a perfect $\{1, a, a^2, b\}$–shift N–design in a group $\mathcal{G}$ exists, then

i) ba^{-1} has even order in $\mathcal{G}$,

ii) a is not on the orbit of ba^{-1},

iii) if $a^{4l_1} = (ba^{-1})^{l_2}$ for some positive integers l_1 and l_2, then $l_1 + 2 \cdot l_2 \equiv 0 \bmod 4$.

iv) $\mathcal{F}$ is the union of the conjugacy classes of the subgroup $< (ba^{-2})^4 >$ generated by the element $(ba^{-2})^4$.

Proof:

i) is immediate from conditions (5) and (6), since $(ba^{-1})^k = (ba)^k \cdot a^{-2k}$ and $2k$ must be divisible by 4.

ii) If $(ba^{-1})^k = a$ for some k, then $b^k = a^{k+1}$, which cannot occur since $2k + 1$ is not divisible by 4 (condition (6)).

iii) follows from condition (6).

iv) If a power of ba^{-2} is contained in $\mathcal{F}$, then by conditions (5) and (6) $(ba^{-2})^k = (ba)^k \cdot a^{-2k}$ can only be a member of $\mathcal{F}$ if k is divisible by 4.

The first nontrivial 4–shift N–design occurs for $N = 12$, i. e., $8N + 1 = 97$. For instance, the set

$$\mathcal{H} = \mathcal{H}_1 \cup \mathcal{H}_2 = \{1, 6, 36, 22, 35, 16\} \cup \{5, 30, 14, 13, 19, 17\}$$

forms a perfect 4–shift 8–design in Z_{97}.

There are only 21 prime numbers $p = 8N + 1 < 25000$ for which a perfect 4–shift N–design exists in Z_p, namely $p =$ 97, 1873, 2161, 3457, 6577, 6673, 6961, 7297, 78730, 10273, 12721, 13537, 13681, 13729, 15601, 15649, 16033, 16561, 16657, 21121, 22129.

Observe that $p = 2161$ is the first number for which as well a perfect 3–shift as a perfect 4–shift design in Z_p exists.

For composite numbers $n = 8N+1$ the conditions on the existence of a perfect 4–shift N–design are similar to the conditions for 3–shift designs (see above). A perfect 4–shift N-design in Z_n, $n = 8N+1$, exists exactly if there exist perfect 4–shift designs in Z_m for all proper divisors m of n and if $\varphi(n) \equiv 0 \pmod 8$ and the conditions of Theorem 1 hold in Z_n^*. The only exception is the trivial design $\{1\}$ in Z_9.

The following table contains the number of primes $p = 2 \cdot |\mathcal{S}| \cdot N + 1$, $N = 1, \ldots, 500$, for which a perfect $\{1, a, \ldots, a^r, b \ldots, b^s\}$–shift design exists in Z_p for some choices of the parameters a and b.

$\frac{r+s+1}{(a,b)}$	3	4	5	6	7	8	9	10
(2,3)	46	4	23	6	12	1	13	8
(2,5)	48	5	22	17	18	1	13	1
(2,7)	48	5	23	9	21	1	17	1
(3,4)	50	1	28	2	19	1	17	1
(3,5)	51	19	32	2	18	11	15	2
(3,7)	46	20	29	3	24	9	16	7
(4,5)	50	2	31	0	17	0	17	1
(4,7)	51	0	28	0	13	0	14	0
(5,7)	49	18	19	15	18	9	15	1

These numbers have been obtained by checking the conditions in Theorem 1 or Corollaries 1 and 2, respectively, for each group Z_p.
The table suggests that the distribution of the shift designs depends on the numbers $r+s+1$. Observe that there are many more shift designs for odd numbers $r+s+1$ than for even numbers. Moreover, if $\gcd(a \cdot b, r+s+1) = 1$, then often there are more shift designs for the same $r+s+1$ as in the opposite case.
Furthermore, it seems as if the number of perfect $\{1, a, \ldots, a^r, b, \ldots, b^s\}$–shift N–designs (denoted as $S(N, a, b)$) for primes of the form $p = 2 \cdot (r+s+1) \cdot N + 1$ asymptotically is a constant $c(a, b)$ times the number of all primes of this form (denoted by π_N), i. e., for all pairs (a, b) computer observations suggest that

$$\lim_{N\to\infty} \frac{S(N, a, b)}{\pi_N} = c(a, b)$$

for some constant $c(a, b)$.
However, such distributions are usually hard to analyze. It is not even clear if there exist infinitely many primes p such that a perfect $\{1, a, \ldots, a^r, b, \ldots, b^s\}$–shift N–design in Z_p exists (for any choice of a, b, r, s).
(Since there exists a perfect 3– shift design for every power of 7 (cf. [1]), there indeed exist infinitely many perfect 3–shift designs).

Acknowledgment

The author wishes to thank Han Vinck for drawing his attention to this problem.

References

[1] V. I. Levenshtein and A. J. Han Vinck, "Perfect (d,k)–codes capable of correcting single peak shifts", *IEEE Trans. Inform. Theory*, vol. 39, no. 2, pp. 656–662, 1993.