

A family of near-optimal cyclic uncoverings

Robert F. Bailey
School of Mathematical Sciences
Queen Mary, University of London
Mile End Road, London E1 4NS
United Kingdom
r.f.bailey@qmul.ac.uk

November 16, 2004

Abstract

We give a proof of a general construction of a $(2m, 3, m - 1)$ -uncovering, which is equivalent to a $(2m, 2m - 3, m - 1)$ -covering design. Furthermore, we calculate the Schönheim Bound explicitly for these parameters, and show that our construction gives uncoverings within a constant factor of this bound. We also give an induced construction for $(2m - 1, 4, m - 2)$ -uncovering.

1 Coverings and uncoverings

Covering designs are a generalisation of t -designs, defined as follows.

Definition 1. Let X be a set of v points, and let $v > k \geq t > 0$. A (v, k, t) -covering design is a set of k -subsets of X , called *blocks*, such that any t -subset of points is contained in at least one block.

A survey article on covering designs can be found in [3], while an extensive database of covering designs can be found in [2]. A related concept is that of an *uncovering*, defined below.

Definition 2. Again, let X be a set of v points, with $v > k > 0$ and $v - k \geq t > 0$. A (v, k, t) -uncovering is a set of k -subsets of X , called *coblocks*, such that any t -subset of points is *disjoint* from at least one coblock.

It follows from the definition that the complements of the blocks from a (v, k, t) -covering design will form the coblocks of a $(v, v - k, t)$ -uncovering, so whenever one has a covering design, a corresponding uncovering can easily be obtained, and vice-versa. Uncoverings have been introduced by the author in [1] as part of a decoding algorithm for error-correcting codes based on sharply k -transitive permutation groups. In particular, a family of $(v, 3, t)$ -uncoverings (with $t < \frac{1}{2}v$) was needed for sharply 3-transitive groups. Section 2 gives a construction for $v = 2m$ points; from this a construction for $2m - 1$ points can be obtained, as described in section 4.

In this article the application to coding theory will not be discussed further: see [1] for details.

2 The construction

We now present our construction of a $(2m, 3, m - 1)$ -uncovering. While this is equivalent to a $(2m, 2m - 3, m - 1)$ -covering design, the proof is in terms of uncoverings. As the coblocks have size three, we refer to them as *triples*.

Theorem 1. *The set of all $2m$ triples of the form $\{i - 1, i, i + m\}$, for $i \in \mathbb{Z}_{2m}$ and with addition modulo $2m$, forms a $(2m, 3, m - 1)$ -uncovering.*

Proof. We'll show that, given an arbitrary $(m - 1)$ -subset of \mathbb{Z}_{2m} , there exists a pair of the form $\{i, i + m\}$ that can be extended to a triple either of the form $\{i - 1, i, i + m\}$ or $\{i, i + m - 1, i + m\}$ that is disjoint from it. This will be done by a recursive procedure.

Let X_1 denote an arbitrary $(m - 1)$ -subset of \mathbb{Z}_{2m} , and let \bar{X}_1 denote its complement. Now, first we want a pair $\{i_1, i_1 + m\} \subset \bar{X}_1$. Since \mathbb{Z}_{2m} can be partitioned into m such pairs, and because $|\bar{X}_1| = m + 1$, then there must exist at least one pair which is wholly contained in \bar{X}_1 . Then there are two possibilities:

- (a) one (or more) of $i_1 - 1, i_1 + m - 1$ lies in \bar{X}_1 , in which case $\{i_1, i_1 + m\}$ can be extended to a triple, so we are done;
- (b) both of $i_1 - 1, i_1 + m - 1$ lie in X_1 , in which case we fail.

In case (b), we know that the pair $\{i_1, i_1 + m\}$ cannot be extended, and so can be excluded, and also that the pair $\{i_1 - 1, i_1 + m - 1\}$ (which has the same form) is contained in X_1 . Thus we can ignore these four points.

Let X_2 denote $X_1 \setminus \{i_1 - 1, i_1 + m - 1\}$, and let \bar{X}_2 denote $\bar{X}_1 \setminus \{i_1, i_1 + m\}$. (Note that this is *not* the complement of X_2 .) Now we know that there are $m - 2$ pairs remaining, and that $|\bar{X}_2| = m - 1$, so there must exist a pair $\{i_2, i_2 + m\} \subset \bar{X}_2$.

If we fail to extend *this* pair, then we can remove it from \bar{X}_2 to form \bar{X}_3 , and we can also remove $\{i_2 - 1, i_2 + m - 1\}$ from X_2 to form X_3 .

We then repeat this procedure, either until an extendable pair is found, or until we get as far as we can go. We consider the cases where m is odd and even separately.

First, suppose m is odd. Then, if we continue to fail at each step, we will ultimately reach $X_s = \emptyset$, where $s = \frac{m-1}{2}$. In which case, both $i_s - 1$ and $i_s + m - 1$ *must* belong to \bar{X} , so therefore the pair $\{i_s, i_s + m\}$ can be extended to a triple as required.

Second, suppose m is even. Then, if no extendable pair is found at an earlier step, we will reach $X_t = \{x\}$ (where $t = \frac{m-2}{2}$). Then at most one of $i_t - 1, i_t + m - 1$ can be equal to x , so therefore this pair can be extended. This completes the proof. \square

Example 1. Consider the case $m = 5$. In each row, the framed elements form a coblock in an uncovering, the remaining elements form a block in the corresponding covering design.

1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10

Note: Examples of these uncoverings (or, more specifically, the corresponding covering designs) appear in [2], as “cyclic coverings found by search program”. No reference for a general construction is given.

3 The Schönheim bound

The Schönheim bound, $L(v, k, t)$, is explained in [3]. It gives a theoretical lower bound on the size of a (v, k, t) -covering design, and thus also a $(v, v - k, t)$ -uncovering,

and is as follows:

$$L(v, k, t) = \left\lceil \frac{v}{k} \left\lceil \frac{v-1}{k-1} \cdots \left\lceil \frac{v-t+1}{k-t+1} \right\rceil \cdots \right\rceil \right\rceil.$$

In general, this is difficult to evaluate, given that it is in terms of three variables and is full of “nested” ceiling functions. In our case, we have $v = 2m$, $k = 2m - 3$ and $t = m - 1$, so we can at least reduce it to a function of just one variable. So we have the following:

$$L(m) = \left\lceil \frac{2m}{2m-3} \left\lceil \frac{2m-1}{2m-4} \cdots \left\lceil \frac{m+2}{m-1} \right\rceil \cdots \right\rceil \right\rceil.$$

The remainder of this section is the proof of the following, rather surprising, theorem.

Theorem 2. *Suppose $m \geq 6$. Then $L(m) = \frac{13}{8}m + c$, where c is a constant depending on congruence classes modulo 8, with $0 \leq c \leq \frac{13}{8}$.*

This result is surprising as if the ceiling functions were not present we would have

$$\frac{2m(2m-1)(2m-2)}{(m+1)m(m-1)} = \frac{8m^3 - 12m^2 + 4m}{m^3 - m} \rightarrow 8 \text{ as } m \rightarrow \infty$$

and not a linear function.

Proof. We begin by defining a recursion as follows:

$$\begin{aligned} f_1 &= 1 \quad (\text{corresponding to the “empty product”}) \\ f_2^* &= \frac{m+2}{m-1} f_1 = \frac{m+2}{m-1}, \quad f_2 = \lceil f_2^* \rceil \\ &\vdots \\ f_l^* &= \frac{m+l}{m+l-3} f_{l-1}, \quad f_l = \lceil f_l^* \rceil \\ &\vdots \\ f_m^* &= \frac{2m}{2m-3} f_{m-1}, \quad f_m = \lceil f_m^* \rceil = L(m). \end{aligned}$$

We assume that m is “large enough”, so that $\frac{m+2}{m-1} \leq 2$ (i.e. so that $f_2 = 2$, which requires $m \geq 4$). Also, we assume that m is “large enough” so that $f_3 = 3$, i.e. that $2\left(\frac{m+3}{m}\right) \leq 3$, which requires $m \geq 6$. (This is the source of the restriction on m .) Observe the differences $f_2 - f_1$ and $f_3 - f_2$ are both 1.

We wish to find the first term in the sequence f_l where the difference $f_{l+1} - f_l \geq 1$. That is, we want the smallest value of l where this holds. We call this value i . Since all previous differences have been 1, we know that $f_i = i$. So we have the inequality:

$$\begin{aligned}
f_{i+1}^* &= \frac{m+i+1}{m+i-2}f_i > f_i + 1 \\
\Leftrightarrow i(m+i+1) &> (i+1)(m+i-2) \\
\Leftrightarrow im+i^2+i &> im+i^2-2i+m+i-2 \\
\Leftrightarrow 0 &> m-2-2i \\
\Leftrightarrow i &> \frac{1}{2}m-1.
\end{aligned}$$

Thus we need to take i to be the least integer exceeding $\frac{1}{2}m - 1$.

- If m is even, then $i = \frac{1}{2}m$.
- If m is odd, then $i = \frac{1}{2}(m - 1)$.

By a similar chain of inequalities, starting with $f_{i+1}^* \leq f_i + 2$, and with our requirement that $m \geq 6$, we have that $f_{i+1} - f_i = 2$. So we now assume that there are several further differences of 2, and that the first difference of greater than 2 occurs at the $(i+j+1)^{\text{th}}$ step. Note that $f_{i+j} = i+2j$. Now we have another chain of inequalities:

$$\begin{aligned}
f_{i+j+1}^* &= \frac{m+(i+j)+1}{m+(i+j)-2}f_{i+j} > f_{i+j} + 2 \\
\Leftrightarrow (i+2j)(m+(i+j)+1) &> (i+2j+2)(m+(i+j)-2) \\
\Leftrightarrow i+2j &> -2i-4j+2m+2i+2j-4 \\
\Leftrightarrow 4j &> 2m-4-i
\end{aligned}$$

Dividing through by 4 and substituting the values of i obtained above, we obtain:

- if m is even, $j > \frac{3}{8}m - 1$;
- if m is odd, $j > \frac{3}{8}m - \frac{7}{8}$.

Thus we must take as our value of j the least integer exceeding these, so we must consider congruence classes modulo 8. The values obtained are given in the table

below.

$m \equiv 0 \pmod{8}$	$j = \frac{3}{8}m$
$m \equiv 1 \pmod{8}$	$j = \frac{3}{8}m - \frac{3}{8}$
$m \equiv 2 \pmod{8}$	$j = \frac{3}{8}m - \frac{3}{4}$
$m \equiv 3 \pmod{8}$	$j = \frac{3}{8}m - \frac{1}{8}$
$m \equiv 4 \pmod{8}$	$j = \frac{3}{8}m - \frac{1}{2}$
$m \equiv 5 \pmod{8}$	$j = \frac{3}{8}m + \frac{1}{8}$
$m \equiv 6 \pmod{8}$	$j = \frac{3}{8}m - \frac{1}{4}$
$m \equiv 7 \pmod{8}$	$j = \frac{3}{8}m - \frac{5}{8}$

By evaluating the inequality $f_{i+j+1}^* \leq f_{i+j} + 3$, we can verify that the difference $f_{i+j+1} - f_{i+j} = 3$.

The next step is to show that there will never be a difference of more than 3, by showing that the first step where this could occur would be after the m^{th} iterate. That is, we show that if the first difference of more than 3 occurs at step $i+j+k+1$, then $i+j+k+1 > m$.

By hypothesis, $f_{i+j+k} = i+2j+3k$. In a similar manner to the above, we have yet another chain of inequalities.

$$\begin{aligned}
 f_{i+j+k+1}^* &= \frac{m+(i+j+k)+1}{m+(i+j+k)-2} f_{i+j+k} > f_{i+j+k} + 3 \\
 \Leftrightarrow (i+2j+3k)(m+(i+j+k)+1) &> (i+2j+3k+3)(m+(i+j+k)-2) \\
 \Leftrightarrow i+2j+3k &> -2i-4j-6k+3m+3i+3j+3k-6 \\
 \Leftrightarrow 6k &> 3m-6-3j \\
 \Leftrightarrow k &> \frac{1}{2}m-1-\frac{1}{2}j \\
 &\text{(substituting } j \leq \frac{3}{8}m + \frac{3}{8}\text{)} \\
 \Leftrightarrow k &> \frac{1}{2}m-1+\frac{3}{16}m-\frac{3}{16} = \frac{5}{16}m-\frac{19}{16}.
 \end{aligned}$$

But $i+j \geq \frac{7}{8}m - \frac{7}{8}$, so we have:

$$\begin{aligned}
 i+j+k+1 &> \frac{7}{8}m - \frac{7}{8} + \frac{5}{16}m - \frac{19}{16} \\
 &= \frac{19}{16}m - \frac{17}{16} \\
 &= m + \frac{3}{16}m - \frac{17}{16} \\
 &> m
 \end{aligned}$$

provided that $3m - 17 > 0$. But we have $m \geq 6$, so this holds.

Thus the remaining $m - (i + j)$ differences must be 3. Hence we can now calculate the values of $f_m = L(m)$. We have:

$$\begin{aligned} f_m &= i + 2j + 3(m - (i + j)) \\ &= 3m - (2i + j). \end{aligned}$$

The values of $f_m = L(m)$ (depending on congruence classes modulo 8) are given in the table below.

	i	j	$2i + j$	$f_m = L(m)$
$m \equiv 0 \pmod{8}$	$\frac{1}{2}m$	$\frac{3}{8}m$	$\frac{11}{8}m$	$\frac{13}{8}m$
$m \equiv 1 \pmod{8}$	$\frac{1}{2}(m - 1)$	$\frac{3}{8}m - \frac{3}{8}$	$\frac{11}{8}m - \frac{11}{8}$	$\frac{13}{8}m + \frac{11}{8}$
$m \equiv 2 \pmod{8}$	$\frac{1}{2}m$	$\frac{3}{8}m - \frac{3}{4}$	$\frac{11}{8}m - \frac{3}{4}$	$\frac{13}{8}m + \frac{3}{4}$
$m \equiv 3 \pmod{8}$	$\frac{1}{2}(m - 1)$	$\frac{3}{8}m - \frac{1}{8}$	$\frac{11}{8}m - \frac{9}{8}$	$\frac{13}{8}m + \frac{9}{8}$
$m \equiv 4 \pmod{8}$	$\frac{1}{2}m$	$\frac{3}{8}m - \frac{1}{2}$	$\frac{11}{8}m - \frac{1}{2}$	$\frac{13}{8}m + \frac{1}{2}$
$m \equiv 5 \pmod{8}$	$\frac{1}{2}(m - 1)$	$\frac{3}{8}m + \frac{1}{8}$	$\frac{11}{8}m - \frac{7}{8}$	$\frac{13}{8}m + \frac{7}{8}$
$m \equiv 6 \pmod{8}$	$\frac{1}{2}m$	$\frac{3}{8}m - \frac{1}{4}$	$\frac{11}{8}m - \frac{1}{4}$	$\frac{13}{8}m + \frac{1}{4}$
$m \equiv 7 \pmod{8}$	$\frac{1}{2}(m - 1)$	$\frac{3}{8}m - \frac{5}{8}$	$\frac{11}{8}m - \frac{13}{8}$	$\frac{13}{8}m + \frac{13}{8}$

We observe that these values satisfy the statement of the theorem. \square

Recall that the actual uncoverings constructed have size $2m$. While we have not proved that these uncoverings (or the corresponding coverings) have minimal size, it does show that they are (approximately) within a constant factor, $\frac{16}{13}$, of the lower bound.

4 An induced construction for point sets of odd size

The construction described in section 2 above only works for a point set of even size. However, it is easy to obtain a $(2m - 1, 3, m - 2)$ -uncovering from a $(2m, 3, m - 1)$ -uncovering, using the following lemma.

Lemma 3. *Let \mathcal{U} be a (v, k, t) -uncovering with point set $\{1, \dots, v\}$, and let \mathcal{W} be the subset of \mathcal{U} obtained by removing all coblocks containing the point v . Then \mathcal{W} is a $(v - 1, k, t - 1)$ -uncovering.*

Proof. Let E be an $(t - 1)$ -subset of $\{1, 2, \dots, v - 1\}$. Since \mathcal{U} is a (v, k, t) -uncovering, there exists a coblock $T \in \mathcal{U}$ disjoint from the t -set $E \cup \{v\}$. Now, clearly T cannot be one of the m -sets containing v . Thus $T \in \mathcal{W}$, and is disjoint from E . Thus \mathcal{W} is a $(v - 1, k, t - 1)$ -uncovering. \square

Corollary 4. *Let \mathcal{U} be a $(2m, 3, m-1)$ -uncovering of \mathbb{Z}_{2m} as described in theorem 1 above, and let \mathcal{W} be the subset of \mathcal{U} obtained by removing all triples containing the point $2m$. Then \mathcal{W} is a $(2m-1, 3, m-2)$ -uncovering.*

Proof. This is merely a special case of lemma 3. \square

When we calculate the Schönheim bound for these parameters, we obtain

$$\left\lceil \frac{2m-1}{2m-4} \left\lceil \frac{2m-2}{2m-5} \cdots \left\lceil \frac{m+1}{m-2} \right\rceil \cdots \right\rceil \right\rceil$$

which is precisely $L(m-1)$, where L is the function in theorem 2. Thus we have a further corollary.

Corollary 5. *The Schönheim lower bound for a $(2m-1, 3, m-2)$ -uncovering is equal to $\frac{13}{8}(m-1) + c$, where c is a constant as in theorem 2.*

Thus when we compare the size of the uncoverings obtained $(2m-3)$ with the Schönheim bound ($\sim \frac{13}{8}m$), once again we have that size of our construction is (approximately) within a constant factor of the lower bound.

References

- [1] R.F. Bailey, Ph.D. thesis, University of London, in preparation.
- [2] D.M. Gordon, *La Jolla Covering Repository*,
<http://www.ccrwest.org/cover.html>.
- [3] W.H. Mills and R.C. Mullin, Coverings and packings, in *Contemporary Design Theory: A collection of surveys*, (eds. J.H. Dinitz and D.R. Stinson), Wiley, 1992, pp. 371–399.