UNIFORMLY REDUNDANT ARRAYS

A. BUSBOOM, H. ELDERS–BOLL, AND H. D. SCHOTTEN
Institut für Elektrische Nachrichtentechnik
Aachen University of Technology (RWTH)
D-52056 Aachen, Germany

(Received 15 July 1997; accepted in revised form 23 December 1997)

Abstract. Uniformly Redundant Arrays (URA's) are two–dimensional binary arrays with constant sidelobes of their periodic autocorrelation function. They are widely agreed upon to be optimum mask patterns for coded aperture imaging, particularly in imaging systems with a cyclic coded mask. In this paper, a survey of all currently known construction methods for URA's is given and the sizes and open fractions of the arrays resulting from each construction method are pointed out. Alternatives to URA's for situations in which a URA does not exist, are discussed.

Keywords: Coded aperture imaging, Correlation arrays, Gamma–ray imaging, X–ray imaging

1. Introduction

Coded aperture imaging (CAI) (Mertz and Young, 1961; Dicke, 1968) has matured as a standard imaging technique in X–ray and γ–ray astronomy. It is capable of combining high angular resolution with good photon collection efficiency by using a mask consisting of transparent and opaque elements placed in front of a position sensitive detector (Figure 1). With a suitable choice of the aperture pattern it is possible to reconstruct the source distribution to be imaged from the coded detector image and to obtain a better signal–to–noise ratio in the presence of quantum noise and detector background noise than with a single pinhole aperture.

An important type of coded aperture imaging instruments are cyclic systems as the one depicted in Figure 1 (Gunson and Polychronopulos, 1976; Fenimore and Cannon, 1978). Let N_x and N_y denote the number of detector pixels in x– and y–direction, respectively. Then the coded mask is of size $2N_x \times 2N_y$ and consists of a 2×2 mosaic of a basic pattern of size $N_x \times N_y$. Using a suitable collimator, it is ensured that only a field of view of $N_x \times N_y$ sky pixels can contribute to the recorded detector image. A source at each sky pixel within the field of view casts a shadow onto the detector which is a cyclically shifted version of the basic mask pattern. The detector image can then be shown to be the periodic crosscorrelation of the source distribution with the aperture array*.

* The aperture array is an array of size $N_x \times N_y$ that is obtained by assigning a 1 to each transparent, and a 0 to each opaque element of one basic pattern of the coded mask.

Experimental Astronomy **8:** 97–123, 1998.

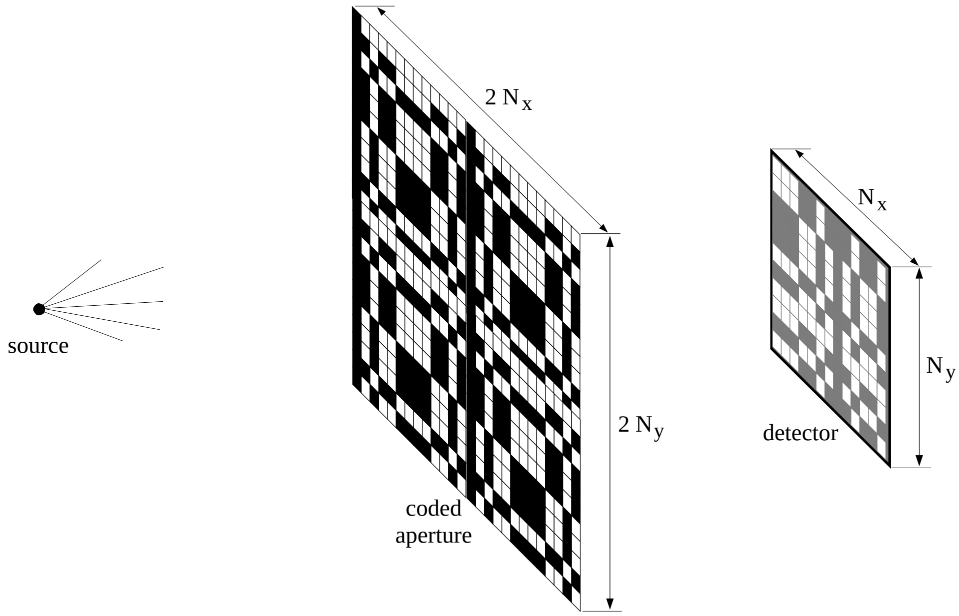


Figure 1. Cyclic coded aperture imaging system.

From among the various algorithms proposed in the literature for reconstructing the original source distribution from the coded detector image, we will only mention two here:

1. For *matched filtering*, reconstruction is achieved by periodically crosscorrelating the detector image with the aperture array itself, possibly scaled by a constant factor and offset by a constant value. Matched filtering can be shown to be optimum with respect to the contribution of quantum noise in the detector measurements to the reconstruction. However, the point spread function (PSF) of the resulting imaging system is the periodic autocorrelation function of the aperture array. Unless this autocorrelation function has constant sidelobe values, the reconstruction will be subject to systematic errors, often referred to as *coding noise* or *artifacts*.
2. For *inverse* or *mismatched filtering*, the detector image is crosscorrelated with the periodic inverse filter of the aperture array (Antweiler and Lüke, 1994; Lüke and Busboom, 1998). In this case, the reconstruction will be free of coding noise for arbitrary aperture arrays, however, amplification of the quantum noise will occur and have a deteriorating effect on the reconstructed image.

Matched and mismatched filtering become identical, except for a constant scaling and offset, if and only if the periodic autocorrelation function of the aperture array has constant sidelobes. Arrays with this property are commonly referred to as *Uniformly Redundant Arrays (URA's).* This term was originally introduced by Fenimore and Cannon (1978) for a particular type of binary arrays with flat periodic autocorrelation sidelobes. Today, however, it is commonly used as a generic term for all binary arrays with this property. URA's are widely agreed upon (Gunson and Polychronopulos, 1976; Fenimore and Cannon, 1978; Skinner, 1984; Busboom et al., 1997b) as being the optimum aperture arrays, at least for cyclic CAI systems, since they combine the advantages of matched filtering (avoidance of quantum noise amplification) and mismatched filter reconstruction (avoidance of systematic coding noise). URA's are also frequently employed as aperture arrays in non–cyclic CAI instruments (Rideout, 1995) even though they are not strictly known to be optimum in any sense in this kind of systems.

An important parameter in the choice of a suitable aperture array is the number of transparent aperture elements or, equivalently, the ratio ρ of open elements to the total number of aperture elements, called *aperture transmission, aperture density,* or *open fraction.* In the literature, there has been a multitude of approaches to the optimization of the open fraction that used different optimization criteria and obtained slightly different results. Gunson and Polychronopulos (1976) optimize the statistical significance of a peak above a constant plateau of background noise. The result is an optimum value for ρ near zero for low background noise and an optimum open fraction near $1/2$ in the background dominant case. Fenimore (1978) maximizes the local signal–to–noise ratio for an individual pixel in the reconstruction. He obtains an open fraction of $1/2$ for high detector background noise and/or strong point sources. For low detector noise and weak or extended sources, Fenimore obtains a lower value for the optimum open fraction but argues that the loss in signal–to–noise ratio is small when a mask with $1/2$ transmission is used nonetheless. A similar approach was taken by Skinner (1984; 1995), however, results differ slightly in that Skinner's optimum open fraction tends toward 1 for low detector background or weak local sources. In 't Zand et al. (1994) refine the analysis by taking into account the non–ideal point spread function of the position sensitive detector. The authors demonstrate that for a finite detector resolution the optimum ρ is lower than that predicted for an ideal detector. For a background dominated situation, they suggest to use a coded mask transmission of $1/3$.

The second important parameter in the aperture design is of course the aperture size $N_x \times N_y$. The choice will usually be governed by technical constraints with respect to the size and resolution of the available detector and by the desired size and resolution of the field of view to be imaged. In many instruments, circular detectors are employed such that square or almost square apertures make the best use of the available detector area. There are, however, situations in which strongly off–square detectors and coded masks are favorable (Rideout, 1995).

In summary, it is desirable in the context of cyclic coded aperture imaging to have a broad choice of Uniformly Redundant Arrays with a variety of sizes, aspect ratios, and open fractions available. Most CAI systems described in the literature make use of a very limited number of families of URA's only while a number of construction methods, some of which have been discovered rather recently, seem not to be widely known in the astronomy community. Also, there have been instances where non–optimum arrays were proposed as aperture arrays even though URA's would have existed for the situations described. It is therefore the purpose of this paper to provide a survey of all currently known construction methods for URA's. Emphasis will be put on the sizes and open fractions of the URA's generated by each construction method.

The remainder of this paper is organized as follows: In Section 2, some important definitions and results from signal theory, finite algebra and design theory are reviewed. As the major theorem of this section we point out an equivalence between URA's and difference sets in abelian, not necessarily cyclic, groups. Section 3 is the main part of this paper, describing the construction methods for URA's in detail. In Section 4 we present invariance operations that allow to generate new URA's of the same size and open fraction from a given URA. This may be desirable for applications in non–cyclic CAI systems since the arrays generated by these invariance operations will vary in their aperiodic autocorrelation properties. Some alternatives to URA's for sizes and/or open fractions for which a URA does not exist or is not known, are discussed in Section 5. Finally, Section 6 comprises an overview of all known URA's up to size 100×100 and some concluding remarks.

2. Definitions and Basic Facts

2.1. Definitions

This paper is mainly concerned with two–dimensional arrays $a(x,\ y); x = 0,\ 1,\ \ldots,\ N_x - 1; y = 0,\ 1,\ \ldots,\ N_y - 1$. An array a will be called a *coherent* binary array if $a(x,\ y) \in \{-1,\ +1\}$, and an *incoherent* binary array if $a(x,\ y) \in \{0,\ 1\}$ for all x and y.

With the 0's and 1's corresponding to opaque and transparent aperture elements, respectively, obviously only incoherent binary arrays can be physically realized as coded masks. If not otherwise stated, the array a is assumed to be an incoherent binary array in the following. The number of 1's in a is denoted by K. With the definition $N = N_x N_y$ the open fraction of a is given by $\rho = K/N$.

The periodic autocorrelation function (PACF) of a is defined as (Lüke, 1992)

$$\tilde{\varphi}_{aa}(l,\ k) = \sum_{x=0}^{N_x-1} \sum_{y=0}^{N_y-1} a(x,\ y)\, a(x + l \bmod N_x,\ y + k \bmod N_y). \tag{1}$$

The values of $\tilde{\varphi}_{aa}$ for $(l,\ k) \neq (0,\ 0)$ are referred to as the *PACF sidelobes* of a. This definition generalizes to one– or to more than two–dimensional arrays in a straightforward manner. As mentioned above, we will use the term Uniformly Redundant Array (URA) for any incoherent binary array a with

$$\tilde{\varphi}_{aa}(l,\ k) = \begin{cases} K & \text{if } (l,\ k) = (0,\ 0), \\ \lambda & \text{otherwise} \end{cases} \tag{2}$$

which is a more general concept than the original definition by Fenimore and Cannon (1978). Obviously, if a is a URA, then the array a' given by $a'(x,\ y) = 1 - a(x,\ y)$ for all x, y also is a URA with open fraction $\rho' = 1 - \rho$. We will therefore restrict this paper to URA's with $\rho \leq 1/2$, bearing in mind that URA's with $\rho > 1/2$ do exist. Also any incoherent binary array with $K = 1$ or $K = N - 1$ trivially is a URA corresponding to a pinhole or "inverse pinhole" aperture. These arrays with not be considered in this paper, either.

2.2. Necessary Existence Criterion

We will make no attempt here to review the abundance of nonexistence proofs for URA's or equivalently, as will be shown in Section 2.5, for difference sets in abelian groups that has been given in the literature. For details the reader is referred to Baumert (1971), Lander (1981), Beth et al. (1985), and the references therein. We will only mention the most important necessary existence criterion that allows to significantly constrain the number of possible URA sizes and open fractions with very little effort.

It can be easily verified that the relation

$$\sum_{l=0}^{N_x-1} \sum_{k=0}^{N_y-1} \tilde{\varphi}_{aa}(l,\ k) = \left[\sum_{x=0}^{N_x-1} \sum_{y=0}^{N_y-1} a(x,\ y) \right]^2$$

holds for any array a. For URA's it follows from Equation (2) that

$$K + \lambda(N - 1) = K^2, \quad \text{i. e.,} \quad \lambda = \frac{K(K-1)}{N-1}. \tag{3}$$

Since a is a binary array, the PACF sidelobe level λ must be an integer. Thus, the most basic feasibility test for the existence of a URA with given N and K is to verify that $K(K - 1)$ is a multiple of $N - 1$.

2.3. Folding and Refolding

Let s be a one–dimensional sequence of length N with PACF $\tilde{\varphi}_{ss}$ (l, k), and let $N = N_x N_y$ where N_x and N_y are coprime. Then the array a given by

$$a(n \bmod N_x,\ n \bmod N_y) = s(n) \quad \text{for all } n = 0,\ 1,\ \ldots,\ N \tag{4}$$

has the periodic autocorrelation function (Lüke, 1992)

$$\tilde{\varphi}_{aa}(m \bmod N_x,\ m \bmod N_y) = \tilde{\varphi}_{ss}(m) \quad \text{for all } m = 0,\ 1,\ \ldots,\ N. \tag{5}$$

The construction of an array from a sequence according to Equation (4) is referred to as *folding*, its inverse, the construction of a sequence from an array is called *refolding*. Since with Equation (5) the PACF's of the sequence and array are related to each other via folding or refolding in the same manner, any one–dimensional URA gives rise to a two–dimensional URA and vice versa, as long as the dimensions N_x and N_y of the two–dimensional array are coprime. Folding and refolding can also be generalized to higher–dimensional arrays in a straightforward manner.

2.4. Basic Facts from Finite Algebra and Design Theory

The purpose of this section is to review only those results from the theory of finite abelian groups and finite fields that will be needed in Section 3 to describe the construction methods for URA's. All theorems will be stated without proof. For details, the reader is referred, e. g., to Baumslag and Chandler (1979) for the theory of finite groups and Lidl and Niederreiter (1983) for the theory of finite fields.

2.4.1. *Finite Abelian Groups*

DEFINITION 2.1. (Baumslag and Chandler, 1979) A *group* is an ordered pair $(G, +)$ of a nonempty set G and a binary operation* $+$ in G if

1. the operation $+$ is associative, i. e.,
   $a + (b + c) = (a + b) + c$ for all $a, b, c \in G$,
2. there exists a zero element $e \in G$ such that
   $a + e = e + a = a$ for all $a \in G$,
3. there exists an inverse element $-a$ for each $a \in G$ such that
   $a + (-a) = (-a) + a = e$.

If, in addition, the operation $+$ is commutative, i. e., $a + b = b + a$ holds for all $a, b \in G$, then $(G, +)$ is called an *abelian group*. The number $|G|$ of elements of G is called the *order* of the group. $(G, +)$ is called a *finite group* if $|G|$ is finite.

DEFINITION 2.2. A group $(G, +)$ of order n is called *cyclic* if there exists an element $a \in G$ such that each $b \in G$ can be expressed as

$$b = ma = \underbrace{a + a + \ldots + a}_{m \text{ terms}}, \quad m \in \{0, 1, \ldots, n-1\}.$$

Note that the zero element is formally written as $0a$. a is called a *generating element* of $(G, +)$.

DEFINITION 2.3. Two groups $(G, +)$, $(H, \star)$ are called *isomorphic* if there is a bijection $f : G \to H$ such that

$$f(a + b) = f(a) \star f(b) \quad \text{for all } a, b \in G.$$

* Note that this operation formally denoted as + does not need to be identical with the standard addition operation

If two groups of the orders n and m are given, then the following theorem allows to construct a new group of order nm, the *direct sum* of the given groups:

THEOREM 2.1. Let $(G, +)$ and $(H, \star)$ be two groups. Let $G \times H$ denote the Cartesian product of G and H, i. e.,

$$G \times H = \{(g, h) \mid g \in G, h \in H\}.$$

Define the binary operation $\cdot$ in $G \times H$ by

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 + g_2, h_1 \star h_2).$$

Then $(G \times H, \cdot)$ is a group of order $|G|\,|H|$. It is called the *direct sum* of $(G, +)$ and $(H, \star)$ and denoted as $(G, +) \oplus (H, \star)$. If $(G, +)$ and $(H, \star)$ are abelian, then their direct sum is also abelian.

The following theorems describe the structure of abelian groups and allow a very general classification:

THEOREM 2.2. Any cyclic group is abelian.

THEOREM 2.3. Cyclic groups exist for all orders $|G| = 1, 2, \ldots$.

THEOREM 2.4. Any two cyclic groups of the same order are isomorphic. For this reason we will also use the term *the cyclic group of order* n in the following, denoted by $C(n)$.

THEOREM 2.5. The direct sum $C(n) \oplus C(m)$ of the cyclic groups of order n and m is cyclic if and only if n and m are coprime.

THEOREM 2.6. Any finite abelian group is isomorphic to the direct sum of a finite number of cyclic groups whose orders are prime powers.

With this theorem, any finite abelian group $(G, +)$ can be represented as

$$(G, +) = C(p_1^{r_1}) \oplus C(p_2^{r_2}) \oplus \ldots \oplus C(p_w^{r_w})$$

where the p_i are prime numbers and $r_i = 1, 2, \ldots$. If the p_i are ordered such that $p_1 \leq p_2 \leq \ldots \leq p_w$ and $r_i \geq r_{i+1}$ if $p_i = p_{i+1}$, then the ordered w–tupel $(p_1^{r_1}, p_2^{r_2}, \ldots, p_w^{r_w})$ is called the *type* of the group $(G, +)$. Note that the type uniquely determines the structure of any finite abelian group which is reflected by the following theorem:

THEOREM 2.7. Two finite abelian groups are isomorphic if and only if they are of the same type.

A special case are finite abelian groups that are the direct sum of cyclic groups whose orders are prime numbers, i. e., $r_1 = r_2 = \ldots = r_w = 1$. A finite abelian group of order n with this property is called the *elementary abelian group of order* n.

2.4.2. *Finite Fields*

DEFINITION 2.4. (Lidl and Niederreiter, 1983) A *field* is an ordered triplet $(F, +, \cdot)$ of a nonempty set F and two binary operations* $+$ and $\cdot$ in F if

1. $(F, +)$ is an abelian group with zero element 0,
2. $(F \setminus \{0\}, \cdot)$ is an abelian group
3. the distributive law holds, i. e.,

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{for all } a, b, c \in F.$$

$(F, +, \cdot)$ is called a *finite field* if $|F|$ is finite.

DEFINITION 2.5. Two fields $(F, +, \cdot)$, $(K, \star, \circ)$ are called *isomorphic* if there is a bijection $f : F \to K$ such that

$$f(a + b) = f(a) \star f(b) \quad \text{and} \quad f(a \cdot b) = f(a) \circ f(b) \quad \text{for all } a, b \in F.$$

The two following theorems contain important results on the existence and uniqueness of finite fields:

THEOREM 2.8. A finite field with q elements exists if and only if q is a prime power.

THEOREM 2.9. Any two finite fields with the same number q of elements are isomorphic.

The finite field with q elements is commonly referred to as the *Galois field* GF(q). For each prime number p the set of integers $\{0, 1, \ldots, p - 1\}$ together with addition and multiplication modulo p form a finite field, the so–called *field of residue classes modulo* p. Due to the uniqueness Theorem 2.9, it is possible to identify the Galois field GF(p) with this field of residue classes modulo p.

The next two theorems describe the structure of the multiplicative and additive group of a finite field:

THEOREM 2.10. The multiplicative group $(F \setminus \{0\}, \cdot)$ of a finite field $(F, +, \cdot)$ is cyclic.

THEOREM 2.11. Let $(F, +, \cdot)$ be a finite field with $q = p^w$ elements, p prime. Then the additive group $(F, +)$ is isomorphic to the elementary abelian group of order q, i. e., to the group $\underbrace{C(p) \oplus C(p) \oplus \ldots \oplus C(p)}_{w \text{ terms}}$.

* Again, note that $+$ and $\cdot$ do not need to refer to the standard addition and multiplication operations.

DEFINITION 2.6. A generating element μ of the multiplicative group $(F \setminus \{0\}, \cdot)$ of a finite field $(F, +, \cdot)$ is called a *primitive element of the field.*

It follows immediately that each element of GF(q) can be uniquely represented as $\mu^j = \underbrace{\mu \cdot \mu \cdot \ldots \cdot \mu}_{j \text{ factors}}$, $j \in \{1, \ldots, q-2\}$ where the zero element 0 of the operation $+$ is formally denoted as $\mu^{-\infty}$ and the neutral element of the operation $\cdot$ is written as μ^0.

DEFINITION 2.7. Let $(F, +, \cdot)$ be a finite field and let $K \subset F$ be a subset of F. If $(K, +, \cdot)$ is a field, then it is called a *subfield* of $(F, +, \cdot)$. $(F, +, \cdot)$ is called an *extension field* of $(K, +, \cdot)$.

THEOREM 2.12. Let GF(p^n) be the Galois field with p^n elements, p prime. Then any subfield of GF(p^n) has p^m elements where m is a divisor of n. For each positive divisor m of n there is exactly one subfield GF(p^m) of GF(p^n) with p^m elements.

While any finite field GF(p) whose number of elements is prime, can be represented as the set of integers $\{0, 1, \ldots, p-1\}$ together with addition and multiplication modulo p, each element of a field GF(p^w) whose number of elements is a prime power (p prime), can be formally written as a polynomial

$$\sum_{i=0}^{w-1} n_i \mu^i, \quad n_i \in \mathrm{GF}(p) \tag{6}$$

of degree $w-1$ in a primitive element μ of GF(p^w). The two operations are the polynomial addition and polynomial multiplication modulo some *primitive polynomial*. Primitive polynomials have been tabulated in the literature, e. g., by Lidl and Niederreiter (1983) and Lüke (1992). They can be generated by search using the property that is must be possible to represent each element of the extension field, with the exception of the zero element, as a power of the primitive element μ.

DEFINITION 2.8. Let q be a prime or a prime power. Consider the Galois field GF(q) and the extension field GF(q^w) (cf. Theorem 2.12). For each $\alpha \in \mathrm{GF}(q^w)$, the *trace of* α *over* GF(q) is defined by

$$\mathrm{Tr}_{\mathrm{GF}(q^w)/\mathrm{GF}(q)}(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{w-1}}.$$

$\mathrm{Tr}_{\mathrm{GF}(q^w)/\mathrm{GF}(q)}(\alpha)$ is always an element of GF(q).

2.5. EQUIVALENCE BETWEEN URA'S AND ABELIAN DIFFERENCE SETS

In this section we introduce the concept of a difference set in a finite group. Difference sets have been extensively studied in the combinatorics literature. Essentially, a difference set is a subset of a group with the property that for each nonzero element of the group there are exactly λ ways of representing it as the difference of two elements of the subset. It will be shown that if the underlying group is abelian, a difference set is equivalent to a, generally multidimensional, Uniformly Redundant Array. Therefore, many results from combinatorics give rise to construction methods for URA's. In fact, the majority of constructions reviewed in this paper was originally published in the context of difference sets, the only exception being the URA's based on perfect binary arrays (Section 3.2). In the latter case the construction methods were first formulated in the context of correlation arrays and gave rise to a family of formerly unknown difference sets.

DEFINITION 2.9. (Beth et al., 1985) Let $(G, +)$ be a finite group of order v. Furthermore, let $D \subset G$ be a nonempty subset of G with $|D| = k$. Then D is called a (v, k, λ)–*difference set in* $(G, +)$ if the list of differences* $d_1 - d_2 \neq 0$, $d_1, d_2 \in D$ contains each nonzero element of G exactly λ times.

If $(G, +)$ is abelian, then D is called an *abelian difference set.*

If $(G, +)$ is cyclic, then D is called a *cyclic difference set.*

An overview of cyclic difference sets was given by Baumert (1971). More recent results as well as results on difference sets in non–cyclic groups can be found in Lander (1981) and Beth et al. (1985). A summary of non–cyclic but abelian difference sets was given by Kopilovich (1989).

THEOREM 2.13. Let $(G, +)$ be a finite abelian group of type $(q_1, q_2, \ldots, q_w)$ where the q_i are prime powers, and let D be a (v, k, λ)–difference set in $(G, +)$. Then there exists a w–dimensional, incoherent binary array a of size $q_1 \times q_2 \times \ldots \times q_w$ such that the PACF of a is given by

$$\tilde{\varphi}_{aa}(l_1, l_2, \ldots, l_w) = \begin{cases} k & \text{if } l_1 = l_2 = \ldots = l_w = 0, \\ \lambda & \text{otherwise.} \end{cases}$$

Proof. Let a_i, $i = 1, 2, \ldots, w$, denote the generating elements according to Definition 2.2 of the cyclic groups $C(q_i)$, respectively. Since $(G, +)$ is the direct sum of the $C(q_i)$, each element $g \in G$ can be represented as

$$g = (x_1 a_1, x_2 a_2, \ldots, x_w a_w), \quad x_i \in \{0, 1, \ldots, q_i - 1\}.$$

Now define the elements of the array a by

$$a(x_1, x_2, \ldots, x_w) = \begin{cases} 1 & \text{if } (x_1 a_1, x_2 a_2, \ldots, x_w a_w) \in D, \\ 0 & \text{otherwise.} \end{cases}$$

* Note that $d_1 - d_2$ is a shorthand notation for $d_1 + (-d_2)$ with $-d_2$ denoting the inverse element of d_2 in $(G, +)$.

Since the difference set D has k elements and each element of a corresponds to exactly one element of G, exactly k elements of a equal one. From this, the main peak of the PACF of a can be immediately seen to be

$$\tilde{\varphi}_{aa}(0,\ 0,\ \ldots,\ 0) = k.$$

The sidelobes of the PACF are given by

$$\begin{aligned}
&\tilde{\varphi}_{aa}(l_1,\ l_2,\ \ldots,\ l_w) \\
&= \sum_{x_1=0}^{q_1-1} \ldots \sum_{x_w=0}^{q_w-1} a(x_1,\ x_2,\ \ldots,\ x_w)\, a(x_1+l_1,\ x_2+l_2,\ \ldots,\ x_w+l_w) \\
&= \sum_{(x_1a_1,\ x_2a_2,\ \ldots,\ x_wa_w)\in D} a(x_1+l_1,\ x_2+l_2,\ \ldots,\ x_w+l_w). \qquad (7)
\end{aligned}$$

Note that the terms in this equation are equal to one if and only if

$$((x_1+l_1)a_1,\ (x_2+l_2)a_2,\ \ldots,\ (x_w+l_w)a_w) \in D,$$

i. e.,

$$(x_1a_1,\ x_2a_2,\ \ldots,\ x_wa_w) + (l_1a_1,\ l_2a_2,\ \ldots,\ l_wa_w) \in D. \qquad (8)$$

Here $(l_1a_1,\ l_2a_2,\ \ldots,\ l_wa_w) \in G \setminus \{0\}$ is a constant, nonzero element of G while $(x_1a_1,\ x_2a_2,\ \ldots,\ x_wa_w) \in D$ takes on each value of D exactly once. With Definition 2.9, the sum in Equation (8) then is an element of D exactly λ times and all PACF sidelobes equal λ. ■

With this result we are now able to exploit known families of abelian difference sets for the construction of Uniformly Redundant Arrays. Note that two–dimensional URA's correspond to difference sets in groups that are the direct sum of two cyclic groups.

In Theorem 2.5 is was stated that the direct sum of two cyclic groups $C(n)$ and $C(m)$ is isomorphic to $C(nm)$ if and only if n and m are coprime. This is analogous to the folding and refolding of arrays described in Section 2.3.

Example. If a difference set exists in $C(15)$, then it corresponds to a one–dimensional URA of length 15. Since $C(15)$ is isomorphic to $C(3) \oplus C(5)$, there must also exist a difference set in the latter group, corresponding to a two–dimensional URA of size 3×5. Equivalently, the two–dimensional URA could be obtained from the one–dimensional URA via folding.

Similar remarks apply to folding and refolding of higher–dimensional arrays or, equivalently, isomorphisms of groups that are the direct sum of more than two cyclic groups. Therefore, difference sets in abelian groups are useful for the construction of two–dimensional URA's as long as the groups they are constructed in are isomorphic to a direct sum of two cyclic groups.

3. Construction Methods for URA's

3.1. Singer URA's

The most important family of difference sets in cyclic groups is based on projective geometries in finite fields (Singer, 1938). In the context of correlation sequences and arrays, these Singer difference sets are equivalent to sequences derived from maximum length shift–register sequences (MacWilliams and Sloane, 1976; Lüke, 1992). They can be described in a very compact way using the trace function.

Let q be a prime or prime power, and consider the Galois field GF(q) and the extension field GF(q^w), $w = 2, 3, \ldots$. Let μ be a primitive element of GF(q^w) such that the nonzero elements of the extension field can be written as μ^n, $n = 0, 1, \ldots, q^w - 2$. Now we define the sequence s of length $(q^w - 1)/(q - 1)$ by

$$s(n) = \begin{cases} 1 & \text{if } \mathrm{Tr}_{\mathrm{GF}(q^w)/\mathrm{GF}(q)}(\mu^n) = 0 \text{ (zero element in GF}(q)), \\ 0 & \text{otherwise,} \end{cases}$$

$$n = 0, 1, \ldots, (q^w - 1)/(q - 1) - 1. \tag{9}$$

The sequence s takes on the value 1

$$K = \frac{q^{w-1} - 1}{q - 1}$$

times, its PACF sidelobes are constant and, with Equation (3), are given by

$$\lambda = \frac{q^{w-2} - 1}{q - 1}.$$

The sequences in Equation (9) can in many cases be folded into two–dimensional arrays. A practically important case is $q = 2$, w even. The sequence length $2^w - 1$ can then be factorized into $(2^{w/2} - 1) \times (2^{w/2} + 1)$. The resulting array dimensions are always coprime such that folding is possible. Furthermore, these arrays are nearly square, a property that is desirable if circular or square detectors are to be employed.

The open fraction of URA's based on Singer difference sets can be seen to be

$$\rho = \frac{q^{w-1} - 1}{q^w - 1}$$

which is approximately $1/q$ for large w, i. e., for large arrays. This property allows the construction of URA's with a rather broad choice of open fractions. In particular, for $q = 2$ arrays with an open fraction of roughly 50% as required for many applications (Fenimore, 1978) can be constructed. Also, for $q = 3$ URA's with $\rho \approx 1/3$ result. Such arrays have been shown to be desirable in situations where the detector resolution is in the order of magnitude of the mask element size (In 't Zand et al., 1994).

3.2. Perfect Binary Arrays

Perfect binary arrays (PBA's) are coherent binary arrays (i. e., arrays with ± 1 elements) whose PACF sidelobes are all zero. If a PBA is transformed into an incoherent binary array by replacing the -1 elements by ones and the $+1$ elements by zeros, or vice versa, the resulting incoherent array has constant, but obviously nonzero, PACF sidelobes. Therefore, in the context of incoherent binary arrays, PBA's are in no respect more "perfect" than other arrays with flat PACF sidelobes, but they do give rise to an important family of URA's that was discovered only several years ago.

It is easy to show that the number of elements of a PBA must be an even square (Lüke, 1992). To date, all known two–dimensional PBA's have aspect ratios of $1:1$ or $1:4$. The first PBA's of size 2×2 and 4×4 were found by Calabro and Wolf (1968). Abelian difference sets pertaining to PBA's of size 6×6, 3×12, and 12×12 were initially described by Spence (1976) and were interpreted as perfect binary arrays by Chan et al. (1979). Further PBA's of size 2×8, 8×8, 4×16, 16×16, 8×32, 6×24, 24×24, and 12×48 were found by Lüke (1987), Jedwab and Mitchell (1988), and Bömer and Antweiler (1990). Finally, Wild (1988) and Jedwab and Mitchell (1990) found a recursive construction method for PBA's of the sizes $3^s 2^r \times 3^s 2^r$ and $3^s 2^{r-1} \times 3^s 2^{r+1}$, $s = 0, 1$; $r = 1, 2, 3, \ldots$ that comprises all currently known two–dimensional PBA's. This method is described in the remainder of this section.

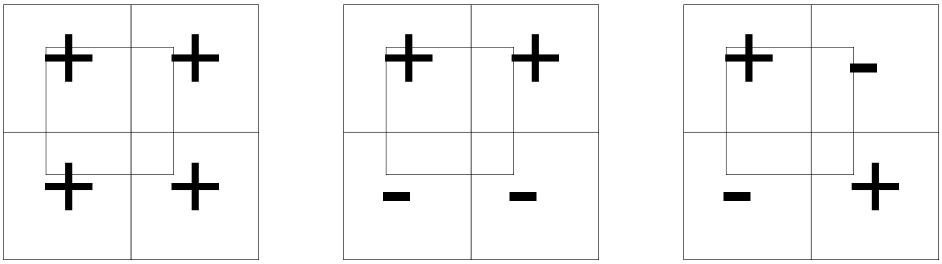
First, the concepts of quasiperiodic and doubly quasiperiodic autocorrelation need to be introduced. Recall that the periodic autocorrelation function (Equation (1)) of an array is computed by shifting the array over a periodically repeated mosaic of itself and by summing up the element–by–element products of the original and shifted array (Figure 2, left). For the quasiperiodic and doubly quasiperiodic autocorrelation functions, the signs of the periodic repetitions of the arrays need to be modified as indicated in Figure 2 (middle and right). We call a coherent binary array quasiperfect (doubly quasiperfect) if its quasiperiodic (doubly quasiperiodic) autocorrelation function vanishes for all nonzero shifts.

Now the recursive construction method is given by the following three theorems:

THEOREM 3.1. (Wild, 1988) Let a be a quasiperfect binary array (QPBA) of size $N_x \times N_x$. Then the array b of size $N_x \times N_x$, defined by

$$b(x, y) = \begin{cases} a(x+y, y) & \text{if } 0 \le x+y < N_x, \\ -a(x+y \bmod N_x, y) & \text{if } N_x \le x+y < 2N_x, \end{cases} \tag{10}$$

is a doubly quasiperfect binary array (DQPBA).



Periodic auto-correlation function — Quasiperiodic auto-correlation function — Doubly quasiperiodic auto-correlation function

Figure 2. Illustration of periodic, quasiperiodic, and doubly quasiperiodic autocorrelation.

THEOREM 3.2. (Jedwab and Mitchell, 1988) Let a be a PBA and b a QPBA, both of size $N_x \times N_x$. Then the array c of size $2N_x \times 2N_x$, defined by

$$c(x,\ y) = \begin{cases} a(x \bmod N_x,\ y/2) & \text{if } y \text{ even,} \\ b(x,\ (y-1)/2) & \text{if } y \text{ odd and } 0 \le x < N_x, \\ -b(x \bmod N_x,\ (y-1)/2) & \text{if } y \text{ odd and } N_x \le x < 2N_x, \end{cases} \tag{11}$$

is a PBA. Furthermore, the array d of size $4N_x \times N_x$, defined by

$$d(x,\ y) = \begin{cases} a(x/2 \bmod N_x,\ y) & \text{if } x \text{ even,} \\ b((x-1)/2,\ y) & \text{if } x \text{ odd and } 0 \le x < 2N_x, \\ -b((x-1)/2 \bmod N_x,\ y) & \text{if } x \text{ odd and } 2N_x \le x < 4N_x, \end{cases} \tag{12}$$

also is a PBA.

THEOREM 3.3. (Jedwab and Mitchell, 1988) Let a be a QPBA and b a DQPBA, both of size $N_x \times N_x$. Then the array c of size $2N_x \times 2N_x$, defined by

$$c(x,\ y) = \begin{cases} a(x/2,\ y \bmod N_x) & \text{if } x \text{ even,} \\ b((x-1)/2,\ y) & \text{if } x \text{ odd and } 0 \le y < N_x, \\ -b((x-1)/2,\ y \bmod N_x) & \text{if } x \text{ odd and } N_x \le y < 2N_x, \end{cases} \tag{13}$$

is a QPBA.

The PBA's of size 2×2 and 6×6:

$$\left|\begin{matrix} + & + \\ + & - \end{matrix}\right| \quad \text{and} \quad \left|\begin{matrix} - & + & + & + & + & - \\ + & - & + & + & + & - \\ + & + & - & + & + & - \\ + & + & + & - & + & - \\ + & + & + & - & + & - \\ + & + & + & + & - & - \\ - & - & - & - & - & + \end{matrix}\right|$$

together with the QPBA's of the same sizes:

$$\begin{vmatrix} + & + \\ + & - \end{vmatrix} \quad \text{and} \quad \begin{vmatrix} + & - & - & + & - & + \\ - & - & - & + & - & + \\ + & + & - & - & + & - \\ - & - & - & - & - & + \\ - & - & - & + & + & + \\ + & + & + & + & - & - \\ + & + & + & - & + & + \end{vmatrix}$$

serve as starting points for the recursive construction method. Assuming a PBA and a QPBA of size $N_x \times N_x$ are known, the recursion consists of three steps:

1. Use Theorem 3.1 to construct a DQPBA of size $N_x \times N_x$ from the given QPBA.
2. Use Theorem 3.2 to construct PBA's of size $2N_x \times 2N_x$ and $4N_x \times N_x$ from the given PBA and QPBA.
3. Use Theorem 3.3 to construct a QPBA of size $2N_x \times 2N_x$ from the given QPBA and the DQPBA generated in step 1. Since now a PBA and a QPBA of size $2N_x \times 2N_x$ are available, the preceding steps can be repeated with $N'_x = 2N_x$.

This recursion allows the construction of PBA's of the sizes mentioned above, with the two exceptions 4×1 and 3×12. These two missing PBA's have the structure:

$$\begin{vmatrix} + & + & + & - \end{vmatrix} \quad \text{and} \quad \begin{vmatrix} - & + & + & - & + & + & + & + & + & - & + & - \\ + & + & + & + & - & + & + & - & + & - & + & - \\ + & + & - & - & + & + & - & - & - & - & - & + \end{vmatrix}.$$

Since the total number of elements of a PBA always is an even square, it can be written as $N = 4l^2$. The incoherent URA's pertaining to PBA's then have the parameters

$$K = l(2l-1), \quad \lambda = l(l-1), \quad \rho = \frac{2l-1}{4l}.$$

For large array sizes, the open fraction ρ can be seen to be approximately 50%. This observation and the fact that many PBA's with exactly square size exist makes them ideal arrays for many coded aperture imaging applications. To the best of our knowledge, however, PBA's have not been practically employed as coded masks yet.

3.3. Quadratic Residue URA's

The term *Uniformly Redundant Arrays* was originally introduced by Fenimore and Cannon (1978) for a family of nearly square binary arrays with flat PACF sidelobes and an open fraction of approximately 50%. Their construction is based upon quadratic residues in Galois fields and was first found by Calabro and Wolf (1968). In this section, we describe a more general construction method that comprises the original URA's and some additional URA's with approximately 50% transmission.

Consider the Galois field GF(p^w), p odd prime, with a primitive element μ. By definition, each nonzero element $\alpha \in$ GF(p^w) can be represented as $\alpha = \mu^j$, $j \in \{0, 1, \ldots, p^w - 2\}$. On the other hand, recall (Equation (6)) that α may be represented by

$$\alpha = \sum_{i=0}^{w-1} x_i \mu^i, \quad x_i \in \{0, 1, \ldots, p-1\}.$$

Obviously, half of the nonzero elements of GF(p^w) are squares, also called *quadratic residues*, that can be written as μ^j with even j. The other half pertains to odd powers of the primitive element. Bömer et al. (1993) have constructed a family of multi–dimensional, ternary arrays from the quadratic residues in GF(p^w):

$$a(x_1, x_2, \ldots, x_w) = \begin{cases} 0 & \text{if } x_1 = x_2 = \ldots = x_w = 0, \\ +1 & \text{if } \sum_{i=0}^{w-1} x_i \mu^i = \mu^j, \ j \text{ even}, \\ -1 & \text{if } \sum_{i=0}^{w-1} x_i \mu^i = \mu^j, \ j \text{ odd}, \end{cases} \tag{14}$$

where $x_i = 0, 1, \ldots, p-1$. Their periodic autocorrelation function can be shown to be

$$\tilde{\varphi}_{aa}(l_1, l_2, \ldots, l_w) = \begin{cases} p^w - 1 & \text{if } l_1 = l_2 = \ldots = l_w = 0, \\ -1 & \text{otherwise}. \end{cases} \tag{15}$$

For $w = 1$, Equation (14) yields the so–called *Legendre sequences* (Lüke, 1992).

Let $q_1 = p_1^{w_1}$ and $q_2 = p_2^{w_2}$ be two powers of odd primes such that $q_2 = q_1 + 2$ and let $a_1(x_1, x_2, \ldots, x_{w_1})$ and $a_2(y_1, y_2, \ldots, y_{w_2})$ be two quadratic residue arrays according to Equation (14) of sizes $p_1 \times p_1 \times \ldots \times p_1$ (w_1 dimensions) and $p_2 \times p_2 \times \ldots \times p_2$ (w_2 dimensions), respectively. For convenience, we combine the indexes $x_1, x_2, \ldots, x_{w_1}$ and $y_1, y_2, \ldots, y_{w_2}$ to the vectors $\mathbf{x}$ and $\mathbf{y}$. A $(w_1 + w_2)$–dimensional URA b can be constructed from a_1 and a_2 by

$$b(\mathbf{x}, \mathbf{y}) = \begin{cases} 0 & \text{if } \mathbf{x} = \mathbf{0}, \\ 1 & \text{if } \mathbf{x} \neq \mathbf{0}, \ \mathbf{y} = \mathbf{0}, \\ 0 & \text{if } \mathbf{x} \neq \mathbf{0}, \ \mathbf{y} \neq \mathbf{0}, \ a_1(\mathbf{x})\, a_2(\mathbf{y}) = +1, \\ 1 & \text{if } \mathbf{x} \neq \mathbf{0}, \ \mathbf{y} \neq \mathbf{0}, \ a_1(\mathbf{x})\, a_2(\mathbf{y}) = -1. \end{cases} \tag{16}$$

This URA is characterized by

$$N = p_1^{w_1}\, p_2^{w_2}, \quad K = \frac{N-1}{2}, \quad \lambda = \frac{N-3}{4}, \quad \rho = \frac{N-1}{2N},$$

its open fraction approaches 50% for large N.

Two–dimensional URA's can be obtained from Equation (16) in three different ways:

1. If $w_1 = w_2 = 1$, then a_1 and a_2 are one–dimensional Legendre sequences and b is a two–dimensional array of size $p_1 \times p_2$. These are the original URA's

according to Calabro and Wolf (1968) and Fenimore and Cannon (1978). This family of URA's is of particular importance for many coded aperture imaging applications since they are nearly square.

2. For $w_1 = 1$ and $w_2 = 2$, b is three–dimensional and has the size $p_1 \times p_2 \times p_2$. By refolding, it can be transformed into a two–dimensional URA of size $p_2 \times p_1 p_2$, i. e., $p_2 \times p_2(p_2 - 2)$.
3. If $w_1 = 2$ and $w_2 = 1$, then b has the size $p_1 \times p_1 \times p_2$. Again, a two–dimensional URA of size $p_1 \times p_1 p_2$, i. e., $p_1 \times p_1(p_1^2 + 2)$, can be obtained by refolding. Note, however, that this case yields only a single array 3×33 for $q_1 = 3^2$ since for all larger q_1, the number $q_2 = q_1 + 2$ cannot be prime.

Note that construction methods 2. and 3. yield strongly off–square URA's.

3.4. McFarland URA's

McFarland (1973) described a family of difference set in non–cyclic, abelian groups. Some of these difference sets give rise to two–dimensional URA's: Let p be an odd prime and consider the group $G = E \oplus K$ where $E = C(p) \oplus C(p)$ and K is an abelian group of order $p + 2$. Note that E is isomorphic to the additive group of the two–dimensional vector space V over the field $GF(p)$. In V there are

$$\frac{p^2 - 1}{p - 1} = p + 1$$

different one–dimensional subspaces which we will denote as $H_1, H_2, \ldots, H_{p+1}$. Furthermore, choose $p + 1$ arbitrary but distinct elements k_i from K. Then a difference set D in G is given by

$$D = \{(h_i,\ k_i) \mid h_i \in H_i,\ i = 1,\ 2,\ \ldots,\ p + 1\}. \tag{17}$$

Since each subspace H_i has p elements, D consists of $K = p(p + 1)$ elements. With Equation (3), we get $\lambda = p$.

Two–dimensional URA's can be obtained from these difference sets in two cases:

1. Let $K = C(p + 2)$ be the cyclic group of order $p + 2$. Then D pertains to a three–dimensional URA of size $p \times p \times p + 2$. Since p and $p + 2$ are always coprime for odd p, this URA can be refolded into a two–dimensional URA of size $p \times p(p + 2)$.
2. If $p + 2$ is not prime, i. e., $p + 2 = n_1 n_2$, $n_1 > 1$, $n_2 > 1$, where n_1, n_2 need not be coprime, then K may alternatively be chosen as the direct sum $K = C(n_1) \oplus C(n_2)$. The corresponding URA then is four–dimensional and of size $p \times p \times n_1 \times n_2$. Since p is prime and thus coprime to both n_1 and n_2, the array can be refolded to a two–dimensional URA of size $pn_1 \times pn_2$. The case that $p + 2$ is a square, i. e., $n_1 = n_2$ is of particular interest since it results in square URA's.

Example. With $p = 7$, the choice $K = C(9)$ yields a URA of size 7×63 while with $K = C(3) \oplus C(3)$, a square URA of size 21×21 can be constructed. Since 7 and 63 are not coprime, these URA's are not equivalent in the sense that they may be converted into each other via folding and refolding.

As can be seen in Figure 5, the number of URA's that can be constructed by this method, is rather sparse. The open fraction is

$$\rho = \frac{p+1}{p(p+2)}.$$

For large arrays, it is of the order $1/p$. Therefore, this construction method is only suitable if URA's with low open fractions are desired for a particular application.

3.5. Other Construction Methods

The construction methods described in the preceding sections comprise almost all currently known two–dimensional URA's. Some additional cyclic difference sets exist that can be regarded as a generalization of quadratic residue arrays (Baumert, 1971). They yield URA's with the parameters $N_y = 3N_x \pm 2$, $k = (N_x N_y - 1)/4$, $\lambda = (N_x N_y - 5)/16$ whose open fraction tends toward 1/4 with increasing array size. These URA's, however, are very rare. The two smallest arrays have the parameters

$$N_x = 7,\ N_y = 19,\ K = 33,\ \lambda = 8,\ \rho = 24.81\%$$

and

$$N_x = 17,\ N_y = 53,\ K = 225,\ \lambda = 56,\ \rho = 24.97\%,$$

the next larger array has $N_x N_y = 6,575,588,101$ elements.

4. Invariance Operations

In coded aperture imaging systems with non–cyclic masks, sometimes referred to as *box cameras*, the *aperiodic autocorrelation function (ACF)* rather than the PACF is relevant for the imaging characteristics. The ACF of an array a is defined by

$$\varphi_{aa}(l,\ k) = \sum_x \sum_y a(x,\ y)\, a(x+l,\ y+k). \tag{18}$$

"Aperiodic URA's", i. e., binary arrays with finite extent whose ACF sidelobes are constant, can not exist. Since no mask patterns are known to date which possess optimum imaging properties in some sense for non–cyclic CAI systems, URA's are frequently employed as coded apertures in such systems (Rideout, 1995).

Several invariance operations are known that allow the construction of new URA's of the same size and open fraction from a given URA. We present three invariance operations here that yield new URA's with the same periodic, but with different aperiodic autocorrelation functions. For the application in non–cyclic CAI systems they allow to choose an aperture array whose ACF is preferable in some sense, from a set of URA's with identical PACF properties (Bömer and Antweiler, 1993).

4.1. Cyclic Shift

Given an array a of size $N_x \times N_y$, the array a' is obtained by

$$a'(x,\ y) = a(x + u \bmod N_x,\ y + v \bmod N_y),$$

$$u = 0,\ 1,\ \ldots,\ N_x - 1, \quad v = 0,\ 1,\ \ldots,\ N_y - 1. \tag{19}$$

The arrays a and a' then have identical periodic autocorrelation functions.

4.2. Stairlike Cyclic Shift

A stairlike cyclic shift of an array a is given by

$$a'(x,\ y) = a(x + uy \bmod N_x,\ y + vx \bmod N_y) \tag{20}$$

where $vN_x \equiv 0 \bmod N_y$ and $uN_y \equiv 0 \bmod N_x$ must hold. In this case, the PACF of a' is obtained from the PACF of a by a similar stairlike cyclic shift. If a is a URA, then a' also is a URA with the same PACF.

4.3. Proper Decimation

Proper decimation is defined as

$$a'(x,\ y) = a(ux \bmod N_x,\ vy \bmod N_y) \tag{21}$$

where u and N_x as well as v and N_y must be coprime. The PACF of a' can be found from the PACF of a by an identical proper decimation. Again, if a is a URA, then a' also is a URA.

5. Variations on the Theme

In the practical design of a coded aperture imaging system, the choice of the mask dimensions and open fraction is typically governed by technical constraints and the desired imaging properties. Constellations may result for which a Uniformly Redundant Array does not exist or is not known. In this section, three possible remedies for this situation are described. They lead to arrays that are not URA's

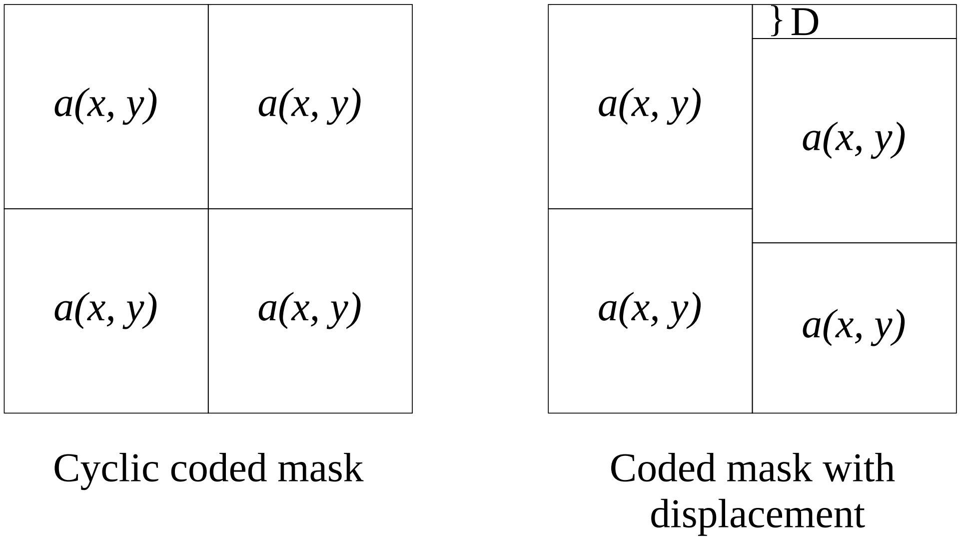


Figure 3. Cyclic and displaced–cyclic coded mask.

in the strict sense but that may have imaging properties close enough to those of URA's to be acceptable for practical purposes.

5.1. Generalized Folding

In a strictly cyclic CAI system, the aperture mask consists of a 2×2 mosaic of a basic pattern (Figure 3, left). This requirement may be relaxed by allowing a periodic displacement in the mask as shown in Figure 3 (right). The right half of the cyclic mask is periodically shifted downward by D elements. With this modification, folding of a sequence into an array can be generalized such that is becomes possible even if the dimensions N_x, N_y of the array are not coprime (Spann, 1965; Lüke and Busboom, 1997). The only constraint is, of course, that the total number of array elements equals the sequence length. The displacement has no negative effect on the imaging properties: The crosscorrelation of a single basic array with the displaced 2×2 mosaic has flat sidelobes granted that the underlying sequence has constant PACF sidelobes.

The simplest implementation of this generalized folding procedure is obtained with $D = N_y - 1$, i. e., a cyclic shift upward by one element. The array a is then obtained from a sequence s by simply arranging the sequence elements along the rows of the array:

$$a\left(n \bmod N_x,\ \left\lfloor \frac{n}{N_x} \right\rfloor \bmod N_y\right) = s(n) \quad \text{for } n = 0,\ 1,\ \ldots,\ N. \qquad (22)$$

In the context of Uniformly Redundant Arrays, the generalized folding can be used to transform the initially one–dimensional sequences constructed from Singer difference sets (Section 3.1) into two–dimensional aperture arrays without any constraints regarding the array dimensions. This gives rise to arrays with some additional sizes and open fractions for which URA's in the strict sense do not exist.

Example. Consider the Singer difference set sequence obtained with $q = 3$, $w = 5$. Its length is $(q^w - 1)/(q - 1) = 121$. Folding according to Equation (4) is not possible since the condition that the array dimensions be coprime cannot be fulfilled. By generalized folding, however, an array of size 11×11 can be constructed:

$$a(x, y) = \begin{vmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{vmatrix} .$$

If the coded mask is designed with a cyclic displacement ($D = 10$), then the resulting aperture has the same perfect imaging properties as a URA of the same size and open fraction.

5.2. Modified Uniformly Redundant Arrays (MURA's)

Gottesman and Fenimore (1989) have proposed a family of correlation arrays that are frequently employed as coded apertures, the so–called *Modified Uniformly Redundant Arrays (MURA's).* This term is somewhat misleading since MURA's do not have constant PACF sidelobes and therefore do not strictly belong to the class of Uniformly Redundant Arrays. Their correlation properties, however, are very close to those of URA's. Furthermore, the facts that MURA's are square, that they exist for many sizes (side lengths must be prime), and that they have an open fraction of approximately 50% make them an interesting alternative to URA's for aperture sizes for which URA's do not exist.

The construction of MURA's is identical to that of the URA's obtained from quadratic residues (Equation (16)). For MURA's, a_1 and a_2 in (16) must be one–dimensional Legendre sequences, both of length q (odd prime). Thus, the condition $q_2 = q_1 + 2$ that was required for URA's, is violated in this case. The resulting arrays are square and have $N = q^2$ elements. They have $K = (N-1)/2$ ones, and their PACF is given by

$$\tilde{\varphi}_{aa}(l,\ k) = \begin{cases} \frac{N-1}{2} & \text{if } (l,\ k) = (0,\ 0), \\ \frac{N-5}{4} & \text{if } (l,\ k) \neq (0,\ 0) \text{ and } a(l,\ k) = 1, \\ \frac{N-1}{4} & \text{if } (l,\ k) \neq (0,\ 0) \text{ and } a(l,\ k) = 0, \end{cases} \tag{23}$$

i. e., their periodic autocorrelation sidelobes take on two values that differ only by one.

As mentioned in Section 1, the inverse filter of a URA with respect to the PACF is identical to the URA itself. Therefore, decoding of the coded detector image is performed by periodically correlating it with the aperture array. If, however, the coded aperture a is a MURA, the detector image needs to be correlated with the inverse filter g which is given by

$$g(x,\ y) = \begin{cases} 1 & \text{if } x = y = 0, \\ a(x,\ y) & \text{otherwise.} \end{cases} \tag{24}$$

From this equation it can be seen that a MURA and its inverse filter differ only by a single element.

Thus, MURA's do not exactly share the optimum property of URA's that the aperture array and its inverse filter have the same structure. This property guarantees that quantum noise in the reconstructed image is minimized while at the same time systematic coding noise is avoided. The deviation of the inverse filter from a MURA is, however, negligibly small, particularly for large array sizes. Since URA's with the same sizes and open fractions as MURA's do not exist*, it can be conjectured that MURA's are in fact optimum aperture arrays for the sizes for that they exist.

5.3. Hexagonal Uniformly Redundant Arrays (HURA's)

All arrays presented so far were defined on a rectangular grid. It is, however, also possible to use hexagonal lattices instead. The generalized folding procedure described in Section 5.1 is also applicable to the mapping of one–dimensional sequences onto a hexagonal array in a straightforward manner. For certain sequence lengths and folding parameters, one basic pattern of the resulting array then has again a hexagonal shape. Note that a necessary condition for this property is that $N \equiv 1 \bmod 6$ holds for the length N of the sequence to be folded. If circular detectors are to be used for recording the coded images, hexagonal arrays use the available detector area more efficiently than rectangular or even square arrays.

* The necessary existence condition from Section 2.2 is violated since $\lambda = (q^2 - 3)/4$. Note that q is odd and can therefore be written as $q = 2k+1$ for some integer k. It follows that $\lambda = k^2+k-1/2$ can not be an integer.

Finger and Prince (1985) explored the folding of quadratic residue sequences with URA properties into hexagonal arrays. They point out that for certain folding parameters, one obtains arrays with practically beneficial symmetry properties. The term *Hexagonal Uniformly Redundant Arrays (HURA's)* was introduced by Finger and Prince for these symmetric arrays with flat PACF sidelobes. Gottesman and Fenimore (1989) extended the analysis to hexagonal arrays derived from one–dimensional MURA's instead of URA's. Practical aspects of the implementation of HURA's in coded aperture imaging systems have been investigated by Cook et al. (1984) and Goldwurm et al. (1990).

5.4. HEURISTIC SEARCH OF NEAR–OPTIMUM ARRAYS

If, due to technical considerations, a coded mask size and open fraction are required for which no URA is known nor one of the remedies discussed in the previous sections can be applied, then the only way of finding a reasonable aperture array is by search. An exhaustive search, i. e., a search comprising *all* binary arrays of a given size and open fraction, would require investigating $\binom{N}{K}$ possible arrays. This, obviously, is not a reasonable option, even if the desired aperture size is moderate, and even if additional symmetry properties are exploited. Therefore, heuristics must be employed to drastically reduce the number of arrays to be searched through in one way or another.

It turns out that the "flatness" of the PACF sidelobes is not a suitable criterion for heuristic search algorithms since arrays that are "close" in the sense that they differ only in few elements are not necessarily "close" with respect to their autocorrelation behavior. On the other hand, the PACF sidelobes are not the most important criterion for the imaging properties of an aperture array, either. If mismatched filtering is used as a reconstruction technique, then the signal energy* of the inverse filter is a measure of the capability of an aperture array to suppress quantum noise in the reconstruction (Busboom et al., 1997a). Uniformly Redundant Arrays have the property that they minimize this signal energy for a given aperture size and open fraction. Using the inverse filter signal energy as an optimization criterion, arrays can be found by heuristic search whose imaging properties are almost as good as those of URA's.

Suitable search strategies are the well–known Simulated Annealing algorithm and variations thereof. These algorithms have in common that in each step a random element of the array is toggled (from one to zero or vice versa). If this change leads to an improvement of the objective function to be optimized, it is always accepted. If the change worsens the objective function, then it is accepted with a probability < 1 only. Large deteriorations of the objective functions are less likely to be accepted than small ones, and during the execution of the algorithm the conditions for accepting a worsening of the objective function become more and more stringent ("cooling" process in Simulated Annealing). Such search algorithms have

* The signal energy of an array is the sum of the squares of the array elements.

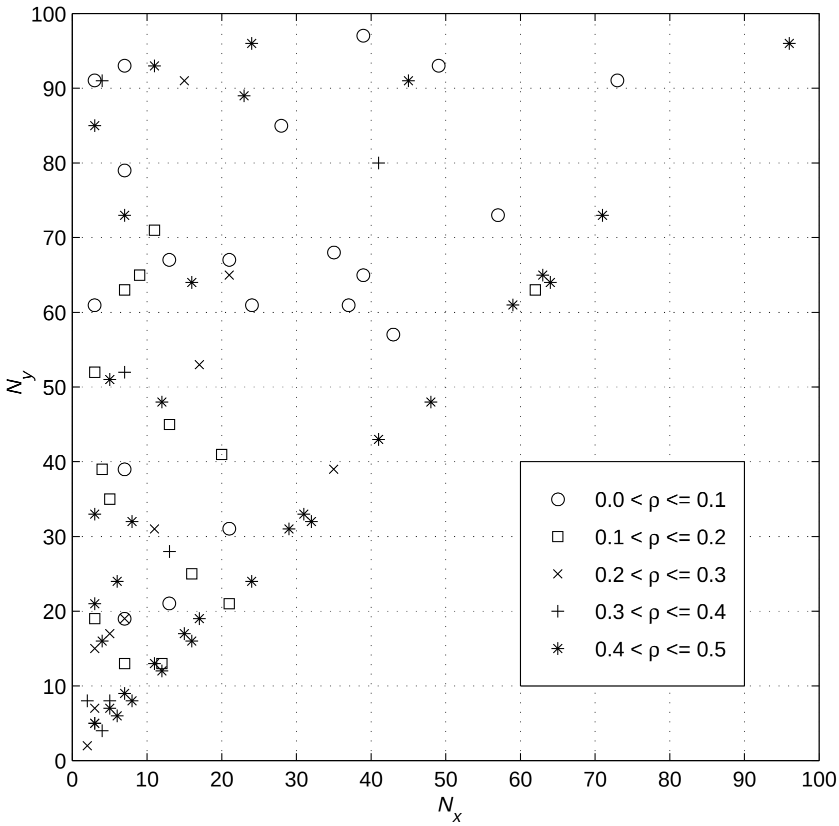


Figure 4. Known Uniformly Redundant Arrays up to size 100 × 100, by open fraction.

the capability of avoiding local extrema of the objective function. For details and search results, the reader is referred to an earlier paper (Busboom et al., 1997a).

6. Summary

It was the intention of this paper to provide the reader with an overview of properties and construction methods for Uniformly Redundant Arrays that are known to be optimum mask patterns for coded aperture imaging. We have attempted to present each construction method as concisely as possible while still being comprehensive enough to enable the reader to implement it without the need for further material. However, readers wishing to apply a particular type of URA in a coded aperture imaging system may wish to refer to the original articles describing the construction method. We have put emphasis on the sizes and open fractions of the URA's that each construction method yields. This should enable the

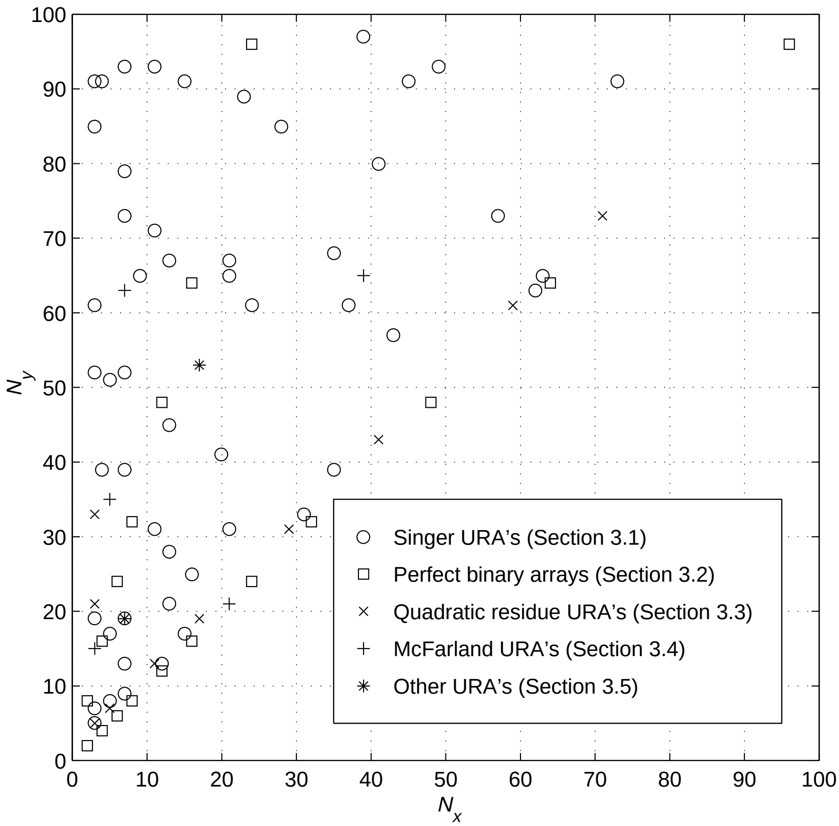


Figure 5. Known Uniformly Redundant Arrays up to size 100 × 100, by construction method.

reader to quickly identify a construction method that is suitable for their particular application.

Figures 4 and 5 summarize the array sizes up to 100 × 100 elements for which URA's are known to exist. In Figure 4 the open fraction is indicated for each array while Figure 5 shows the construction method used to obtain each URA.

The construction methods discussed in this paper comprise, to the best of our knowledge, all currently known two–dimensional binary arrays with flat PACF sidelobes. While for many sizes it has been proven that a URA cannot exist, there remains a large number of sizes for which the question of existence of a URA is open (the smallest size being 8 × 12). We do suspect, however, that the construction methods presented here actually comprise the vast majority of Uniformly Redundant Arrays.

For the case that an aperture size and open fraction is required due to technical considerations for which no URA exists or is known, we have presented three alternatives to URA's. The generalized folding introduced in Section 5.1 only requires a slight modification of the aperture mosaicking and preserves the optimum imaging properties of URA's. The two other alternatives, MURA's and heuristic search, lead to arrays that do not have strictly constant PACF sidelobes but whose imaging properties may be indiscernibly close to those of Uniformly Redundant Arrays for practical purposes.

References

Antweiler, M., and Lüke, H.D.: 1994, 'Mismatched–Filterung periodischer Binärarrays', *Frequenz* **48**, 58–65.

Baumert, L.D.: 1971, *Cyclic Difference Sets* (Springer–Verlag, New York).

Baumslag, B., and Chandler, B.: 1979, *Theory and Problems of Group Theory* (McGraw–Hill, New York, NY).

Beth, T., Jungnickel, D., and Lenz, H.: 1985, *Design Theory* (Bibliographisches Institut, Mannheim).

Bömer, L., and Antweiler, M.: 1989, 'Two–dimensional binary arrays with constant sidelobes in their PACF', *Proc. IEEE Int. Conf. Acoust., Speech, Signal Processing* (Institute of Electrical and Electronics Engineers, Piscataway, NJ), pp. 2768–2771.

Bömer, L., and Antweiler, M.: 1990, 'Two–dimensional perfect binary arrays with 64 elements', *IEEE Trans. Inf. Theory* **36**, 411–414.

Bömer, L., Antweiler, M., and Schotten, H.: 1993, 'Quadratic residue arrays', *Frequenz* **47**, 190–196.

Bömer, L., and Antweiler, M.: 1993, 'Optimizing the aperiodic merit factor of binary arrays', *Signal Processing* **30**, 1–13.

Busboom, A., Elders–Boll, H., and Schotten, H.D.: 1997a, 'Combinatorial design of near–optimum masks for coded aperture imaging', *Proc. IEEE Int. Conf. Acoust., Speech, Signal Processing* (Institute of Electrical and Electronics Engineers, Piscataway, NJ), pp. 2817–2820.

Busboom, A., Schotten, H.D., and Elders–Boll, H.: 1997b, 'Coded aperture imaging with multiple measurements', *J. Opt. Soc. Am. A* **14**, 1058–1065.

Calabro, D., and Wolf, J.K.: 1968, 'On the synthesis of two–dimensional binary arrays with desirable correlation properties', *Inform. Contr.* **11**, 537–560.

Chan, Y.K., Siu, M.K., and Tong, P.: 1979, 'Two–dimensional binary arrays with good autocorrelation', *Inform. Contr.* **42**, 125–130.

Cook, W.R., Finger, M., Prince, T.A., and Stone, E.C.: 1984, 'Gamma–ray imaging with a rotating hexagonal uniformly redundant array', *IEEE Trans. Nucl. Sci.* **31**, 771–775.

Dicke, R.H.: 1968, 'Scatter–hole cameras for x–rays and gamma rays', *Astrophys. J.* **153**, L101–L106.

Fenimore, E.E., and Cannon, T.M.: 1978, 'Coded aperture imaging with uniformly redundant arrays', *Appl. Opt.* **17**, 337–347.

Fenimore, E.E.: 1978, 'Coded aperture imaging: predicted performance of uniformly redundant arrays', *Appl. Opt.* **17**, 3562–3570.

Finger, M.H., and Prince, T.A.: 1985, 'Hexagonal uniformly redundant arrays for coded–aperture imaging', *Proc. 19th Int. Cosmic Ray Conf.* (Scientific and Technical Information Branch, NASA, Washington, DC), pp. 295–298.

Goldwurm, A., and Byard, K., and Dean, A.J., and Hall, C.J., and Harding, J.S.J.: 'Laboratory images with HURA coded apertures', *Astron. Astrophys.* **227**, 640–648.

Gottesman, S.R., and Fenimore, E.E.: 1989, 'New family of binary arrays for coded aperture imaging', *Appl. Opt.* **28**, 4344–4352.

Gunson, J., and Polychronopulos, B.: 1976, 'Optimum design of a coded mask X–ray telescope for rocket applications', *Mon. Not. R. astr. Soc.* **177**, 485–497.

In 't Zand, J.J.M., Heise, J., and Jager, R.: 1994, 'The optimum open fraction of coded apertures', *Astron. Astrophys.* **288**, 665–674.

Jedwab, J., and Mitchell, C.: 1988, 'Constructing new perfect binary arrays', *Electron. Lett.* **24**, 650–652.

Jedwab, J., and Mitchell, C.: 1990, 'Infinite families of quasiperfect and doubly quasiperfect binary arrays', *Electron. Lett.* **26**, 294–295.

Kopilovich, L.E.: 1989, 'Difference sets in noncyclic abelian groups', *Cybernetics* **25**, 153–157.

Lander, E.S.: 1981, 'Symmetric designs and self–dual codes', *Journal of the London Mathematical Society* **24**, 193–204.

Lidl, R., and Niederreiter, H.: 1983, *Finite Fields* (Addison–Wesley, Reading, MA).

Lüke, H.D.: 1987, 'Zweidimensionale Folgen mit perfekten periodischen Korrelationsfunktionen', *Frequenz* **41**, 131–137.

Lüke, H.D.: 1992, *Korrelationssignale* (Springer–Verlag, New York).

Lüke, H.D., and Busboom, A.: 1997, 'Binary arrays with perfect odd–periodic autocorrelation', *Appl. Opt.* **36**, 6612–6619.

Lüke, H.D., and Busboom, A.: 1998, 'Mismatched filtering of periodic and odd–periodic binary arrays', *Appl. Opt.*, **37**, 856–864.

MacWilliams, F., and Sloane, N.J.A.: 1976, 'Pseodo–random sequences and arrays', *Proc. IEEE* **64**, 1715–1729.

McFarland, R.L.: 1973, 'A family of difference sets in non–cyclic groups', *J. Comb. Th. (A)* **15**, 1–10.

Mertz, L., and Young, N.O.: 1961, 'Fresnel transformations of images', *Proc. Int. Conf. Optical Instruments and Techniques* (Chapman and Hall, London), p. 305.

Rideout, M.R.: 1995, *Coded Imaging Systems for X–ray Astronomy* (PhD thesis, University of Birmingham).

Singer, J.: 1938, 'A theorem in finite projective geometry and some applications to number theory', *Trans. Amer. Math. Soc.* **43**, 377–385.

Skinner, G.K.: 1984, 'Imaging with coded–aperture masks', *Nucl. Instr. and Meth.* **221**, 33–40.

Skinner, G.K., and Ponman, T.J.: 1995, 'Inverse problems in x–ray and gamma–ray astronomical imaging', *Inverse Problems* **10**, 655–676.

Spann, R.: 1965, 'A two–dimensional correlation property of pseudorandom maximal length sequences', *Proc. IEEE* **53**, 2137.

Spence, E.: 1977, 'A family of difference sets', *J. Comb. Th. (A)* **22**, 103–106.

Wild, P.: 1988, 'Infinite families of perfect binary arrays', *Electron. Lett.* **24**, 845–847.