UNIVERSITY OF CALIFORNIA AT BERKELEY

DEPARTMENT OF COMPUTER SCIENCE AND ELECTRICAL ENGINEERING

CS-294-6 COMPUTATIONAL IMAGING

HWP 3 **Handed out: 2002 Apr 10th Due: 2002 Apr 17th**

Problem 1: Uniformly redundant arrays (URAs) of size $r \times s$ can be constructed using quadratic residues if r and s is a twin prime pair (i.e. r and s are primes and $r = s + 2$).

The Legendre symbol

$$\left(\frac{k}{n}\right)$$

is defined to be $+1$ when k is a quadratic residue mod n (i.e. if there exists i such that $k = i^2 (\text{mod } n)$), and -1 if k is not a quadratic residue The Legendre symbol has value 0 if k is divisible by n, e.g. if $k = 0$. (See MathWorld web site for additional details if needed).

Define the array A_{ij} as follows:

$$A_{ij} = \begin{cases} 0 & \text{if } i = 0 \\ 1 & \text{if } j = 0 \text{ and } i \neq 0 \\ 1 & \text{if } \left(\frac{i}{r}\right)\left(\frac{j}{s}\right) = +1 \\ 0 & \text{if } \left(\frac{i}{r}\right)\left(\frac{j}{s}\right) = -1 \end{cases}$$

(a) Construct a URA for $r = 7$ (rows) and $s = 5$ (columns). What is the fill factor?

(b)] Check whether the array is self decoding, that is, whether its (two-d) cyclical autocorrelation is two valued — a peak for no shift and a constant pedestal value for non-zero shifts (for shifts less than r horizontally and less than s vertically).

(c) Now repeat the above construction for $r = 5$ (rows) and $s = 7$ (columns). What is the fill factor?

(d) Is the array so created self decoding (check horizontal as well as vertical shifts)? If not, see whether changing the top left element converts the array to one that *is* self decoding.

Hint: complementing a URA ($A'_{ij} = 1 - A_{ij}$) should create a new array that is self-decoding. Similarly, transposing a URA ($A'_{ij} = A_{ji}$) should produce a new array that is self-decoding.

Problem 2: Suppose we want a square rather than rectangular shape for the coding mask. So-called "Modified" uniformly redundant arrays (MURA) can used in this case.

(a) Construct a MURA for $r = 7$ and $s = 7$ using the rule given above for constructing a twin prime URA. Check whether the array so constructed is self-decoding. Check horizontal as well as vertical shifts.

(b) If it is self-decoding, in what way does it differ from the above?

If it is not self decoding, can it be made self decoding by changing the top-left element? Alternatgively, can a decoding mask be made for it by copying the array, then modifying its top-left element?

Problem 3: Suppose a self-decoding array of length N has N_1 1s and N_0 0s (with $N = N_0 + N_1$), and two auto-correlation levels: N_1 (when aligned) and N_2 (when not aligned).

(a) Now instead of using the mask itself for decoding, use a decoding mask obtained by replacing 1s with a and 0s by b. Show that the two levels now are $N_1 a$ and $N_2 a + (N_1 - N_2) b$

(b) What should b in terms of a so that the "background" becomes zero?

(c) If in addition we want the result to be 1 when the decoding mask is lined up with the array, then what should the values of a and b be?

(d) For a one-d array generated using the quadratic residue method,

$$N_1 = (N-1)/2 \quad \text{and} \quad N_2 = (N-1)/4$$

Show that in this case

$$a = (N-1)/4 \quad \text{and} \quad b = -(N-1)/4$$

Problem 4: The cyclical correlation of two sequences of length N is also of length N and can be computed in $O(N^2)$ operations, since each of the N values in the result is the sum of N products. Since correlation is just convolution with the second argument reversed, and since the Fourier transform of a convolution of two functions is the product of the Fourier transforms of the two functions, it would appear that the computation could be speeded up by taking the Discrete Fourier transform (DFT) of the two functions (after reversing one of them), forming the term by term product, and finding the inverse Fourier transform of the result. If we could use the fast Fourier transform (FFT) we should be able to cut the number of operations to order $O(N \log N)$.

However, the FFT only applies when N is composite — and has its maximum speedup only when N is a power of 2 — while methods for producing coding masks with ideal properties only exists for certain N, including prime numbers or products of twin primes.

We could pad out the mask array of length N with zeros until its length is a power of two, $M = 2^n$ say, but then the cylical correlation would have period M, not N, as required.

(a) Show how repeating one of the two sequences and discarding part of the result allows one to compute a cyclical correlation or convolution of two sequences of length N using an array of length $M \geq 2N$.

Now consider computing the FFT of the two sequences — where one has been repeated — after extending them with zeros to a length which is the the nearest larger power of 2, for $2^n \geq 2N$.

(b) What is the worst case ratio of the length of the array needed when computing the FFT for cyclical correlation to the length of the cyclical sequence itself?

(c) How large must N be before the FFT approach starts to pay off in terms of computational complexity? Keep in mind that two forward and one inverse FFT are needed. Also note that the Fourier transform and its inverse require complex arithmetic, and a complex multiplication takes four real multiplications.

Problem 5: Here we prove a remarkable property of quadratic residue masks. Suppose the mask size is p, a prime.

(a) Show that

$$\left(\frac{n-k}{n}\right) = +\left(\frac{k}{n}\right) \quad \text{for} \quad p = 4n+1$$

$$\left(\frac{n-k}{n}\right) = -\left(\frac{k}{n}\right) \quad \text{for} \quad p = 4n+3$$

That is, the cyclical sequence generated using the Legendre symbol is even when p is a prime of the form $4n+1$, while it is odd when p is a prime of the form $4n+3$.

Correspondingly, the Disrete Fourier Transform (DFT) will be real for $p = 4n+1$ and (purely) imaginary for $p = 4n+3$.

(b) Show that if $\{A_l\}$ is the DFT of $\{a_k\}$, then

$$A_l^2 = \begin{cases} +p & \text{when } p = 4n+1 \\ -p & \text{when } p = 4n+3 \end{cases}$$

Hint: if

$$A_l = \sum_{k=0}^{p-1} a_k e^{-j\frac{2\pi kl}{p}}$$

then

$$A_l^2 = \sum_{i=0}^{p-1} a_i e^{-j\frac{2\pi il}{p}} \sum_{j=0}^{p-1} a_j e^{-j\frac{2\pi jl}{p}} = \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} a_i a_j e^{-j\frac{2\pi(i+j)l}{p}}$$

Then separately consider the terms (i) along the diagonal $i = j$, the (ii) cross diagonal $i + j = p$, and (iii) the remainder. For $p = 4n + 3$, these add up to -1, $-(p-1)$, and 0, respectively, while for $p = 4n + 1$, they add up to -1, $(p-1)$, and 2.

Note: this doesn't quite prove the amazing property:

$$A_l = \begin{cases} \sqrt{p}\,a_l & \text{when } p = 4n+1 \\ -j\sqrt{p}\,a_l & \text{when } p = 4n+3 \end{cases}$$