AN ABSTRACT OF THE THESIS OF

Glenn Russell Ruby for the degree of Master of Science

in Computer Science presented on June 4, 1982

Title: An Algebraic View of the Symmetry of Fast Transforms

Abstract approved: Redacted for Privacy

Dr. Paul Cull

Why are the fast Fourier transform and the fast Hadamard transform fast? A transform can be computed by multiplying a matrix times a vector, which normally requires $O(n^2)$ operations. The matrices corresponding to these transforms can be rearranged to eliminate redundant computations resulting in O(nlogn) operations.

We investigate algebraic reasons for fast transforms. Specifically, we notice that these fast transform matrices correspond to the multiplication tables of particular rings. We demonstrate sufficient conditions involving the decomposition of a ring into a descending chain of subrings and a corresponding ascending chain of annihilator subrings. These conditions allow the ring's multiplication table to be arranged in a form which is tiled with variations of a single subblock. We need conditions to insure that the mapping from the ring table to the transform matrix will preserve the subblock structure. One sufficient condition, motivated by the Fourier transform, is that the mapping is a homomorphism. Another sufficient condition, motivated by the Hadamard transform, is that the ring has an orthogonal basis. We display other rings satisfying these conditions or a mixture of these conditions which produce fast transform matrices.

Our conditions are only sufficient: they give a proper subset of the transform matrices representable by the generalized Kronecker product of Fino and Algazi. However, our conditions can describe all commonly used transforms.

An Algebraic View of the Symmetry of Fast Transforms

by

Glenn Russell Ruby, Jr.

A THESIS

submitted to

Oregon State University

in partial fulfillment of
the requirements for the
degree of
Master of Science

Completed June 4, 1982

Commencement June 1983

APPROVED:

Redacted for Privacy

Associate Professor of Computer Science
in charge of major

Redacted for Privacy

Head of Department of Computer Science

Redacted for Privacy

Dean of Graduate School

Date thesis is presented June 4, 1982

Typed by Glenn Russell Ruby, Jr.

TABLE OF CONTENTS

LIST OF FIGURES

An Algebraic View of the Symmetry of Fast Transforms

Chapter I

Introduction

Fast multiplication of a discrete transform matrix times a column vector depends on recognizing and eliminating redundant computations. Normal multiplication will require $O(n^2)$ multiplications and additions. However, the well known fast Fourier and fast Hadamard transforms require only O(nlogn) operations and the fast Haar transform requires only O(n) operations. These transform matrices all share the property of being able to be rearranged by column and row permutations into recursive forms with redundant computational blocks. If we define T(n) as the number of operations needed to multiply an nxn matrix times a column vector, then these recursive forms lead to computational cost recurrence relations $T(n) = 2*T(n/2) + O(n)$ and $T(n) = 2*T(n/2) + O(1)$, giving us the fast O(nlogn) and O(n) computation times (see appendix) .

For the reader unfamiliar with algebraic terminology used in this thesis, definitions may be found in the appendices.

We shall examine the fast Fourier and Hadamard transforms as examples to see what algebraic properties are related to their fast recursive formulations.

The fast Fourier transform as popularly introduced with the Cooley-Tukey algorithm lends itself to fast computation, but perhaps obscure interpretation. Given a discrete Fourier transform matrix of order n where n is highly composite, we can compute the transform product in a sequence of stages, one for each factor. The finite Fourier matrix has the form

(1) $W = [\, w^{ij} \,] \quad i,j = 0,..,n-1$ where w is a principal nth root of unity.

Given a vector A, the transformed vector X is given by

(2) $$X(j) = \sum_i w^{ij} * A(i) \qquad j=0,1,\ldots,n-1$$

The Cooley-Tukey algorithm identifies and eliminates redundant computations in stages as follows. For each factor s of the order n of the matrix, we have a stage of the algorithm. Since n= r*s, for some r, we can interpret the indices in (2) as

$$j = j_1 * r + j_0, \qquad j_0=0,\ldots,r-1, \qquad j_1=0,\ldots,s-1$$

$$i = i_1 * s + i_0, \qquad i_0=0,\ldots,s-1, \qquad i_1=0,\ldots,r-1$$

We can now rewrite (2) as

(3) $$X(j_1,j_0) = \sum_{i_0} \sum_{i_1} w^{ji_1s} * w^{ji_0} * A(i_1,i_0)$$

Since w is an nth root of unity, i.e. $w^{r*s} = w^n = 1$, we can eliminate redundant computations by observing that

$$w^{ji_1s} = w^{j_0i_1s}$$

so that the inner sum over i_1 no longer depends on j_1, but only on j_0 and i_0. We can now write the inner sum as

$$A_1(j_0,i_0) = \sum_{i_1} w^{j_0i_1s} * A(i_1,i_0)$$

and rewrite (3) as

$$X(j_1,j_0) = \sum_{i_0} w^{(j_1 r+j_0)i_0} * A_1(j_0,i_0)$$

Vector A_1 has n components as j_0 and i_0 run through their ranges, with each component being a sum over i_1, for a total of n*r operations. Vector X has again n components with the sum over i_0 for each component, so that X requires n*s operations to compute. The time required for a single stage becomes n(r+s) rather than n(r*s). Consequently, if $n = r^k$, the time for the algorithm will become $n*(r\log_r n)$.

For our purposes it is more useful to observe the structure of the recursive formulation of the finite Fourier matrix. For simplicity assuming $n = 2^k$, label the column indices of the Fourier matrix of order n with numbers from 0 to n-1 in a k place binary format with leading zeroes if necessary. Now, reverse each binary number string representing a column position and permute the columns to the position determined by the value of the reversed binary number. This gives us the following recursive form of the Fourier matrix :

$$F_n = \begin{bmatrix} F_{n/2} & D_{n/2} F_{n/2} \\ F_{n/2} & -D_{n/2} F_{n/2} \end{bmatrix}$$

The diagonal matrices $D_{n/2}$ have elements w^i in the ith row and column. The matrices $F_{n/2}$ are exactly the (correctly permuted) recursive Fourier matrices of order n/2, since

w^2 is an n/2 root of unity and the bit reversal has given the proper arrangement for the recursive form.

Our guide in observation will be the multiplication table of the ring Z_n corresponding to the row and column indices of the recursive Fourier matrix, with the product entries corresponding to the powers of w of the recursive Fourier matrix. Looking at figure 1, we notice that the arrangement of the columns of the table can be interpreted as the successive coset decomposition of a chain of subrings, $Z_n=S_0 \supset S_1 \supset S_2 \supset \ldots \supset S_k$, (in fact ideals) of Z_n. The row arrangement is determined by a corresponding chain of annihilator subrings, $\{0\} \subset A_1 \subset A_2 \subset \ldots \subset A_k \subset Z_n$, (again ideals) where all the elements of A_i annihilate the elements of S_i. Instead of a coset breakdown of the rows, we choose an 'inverted' ordering building in 'top down' fashion a listing of the table's row entries by using at each stage elements of the current annihilator subring serving in the role of coset leaders. Starting with A_1, spread the elements of A_1 evenly down the list, (in this case, 0 in position 0, and 8 in position 8). Pick from A_2 a set of representative coset leaders of A_1 factoring A_2, spreading these leaders evenly between the 0 in position 0 and the next previously placed element of A_1. These same leaders are then similarly spread after each of the remaining elements of A_1 in the list. Repeat this same process with A_j factoring A_{j+1}, finishing with A_k factoring the entire ring R. The value at a given row

Figure 1. Multiplication table factorization of ring Z_{16} for the discrete Fourier transform of order 16.

					<2>								1+<2>							
					<4>				2+<4>											
					<8>		4+<8>													
A_1	A_2	A_3	L_3		0	8	4	12	2	10	6	14	1	9	5	13	3	11	7	15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
			1	1	0	8	4	12	2	10	6	14	1	9	5	13	3	11	7	15
		2	0	2	0	0	8	8	4	4	12	12	2	2	10	10	6	6	14	14
			1	3	0	8	12	4	6	14	2	10	3	11	15	7	9	1	5	13
	4	0	0	4	0	0	0	0	8	8	8	8	4	4	4	4	12	12	12	12
			1	5	0	8	4	12	10	2	14	6	5	13	9	1	15	7	3	11
		2	0	6	0	0	8	8	12	12	4	4	6	6	14	14	2	2	10	10
			1	7	0	8	12	4	14	6	10	2	7	15	3	11	5	13	1	9
8	0	0	0	8	0	0	0	0	0	0	0	0	8	8	8	8	8	8	8	8
			1	9	0	8	4	12	2	10	6	14	9	1	13	5	11	3	15	7
		2	0	10	0	0	8	8	4	4	12	12	10	10	2	2	14	14	6	6
			1	11	0	8	12	4	6	14	2	10	11	3	7	15	1	9	13	5
	4	0	0	12	0	0	0	0	8	8	8	8	12	12	12	12	4	4	4	4
			1	13	0	8	4	12	10	2	14	6	13	5	1	9	7	15	11	3
		2	0	14	0	0	8	8	12	12	4	4	14	14	6	6	10	10	2	2
			1	15	0	8	12	4	14	6	10	2	15	7	11	3	13	5	9	1

where the column subring factorization chain

Z_{16} S_1 S_2 S_3 is defined by

$S_1 = \langle 2 \rangle = \{0,2,4,6,8,10,12,14\}$

$S_2 = \langle 4 \rangle = \{0,4,8,12\}$

$S_3 = \langle 8 \rangle = \{0,8\}$

where the row annihilator subring factorization chain

$\{0\}=A_0$ A_1 A_2 A_3 is defined by

$A_1 = \langle 8 \rangle = \{0,8\}$

$A_2 = \langle 4 \rangle = \{0,4,8,12\}$

$A_3 = \langle 2 \rangle = \{0,2,4,6,8,10,12,14\}$

where L_3 is a set of coset leaders of A_3 in Z_{16}

$L_3 = \{0,1\}$

position is the sum of the elements which designate that position. For example, from figure 1, element 11 is the sum of 8 from A_1, 0 from A_2, 2 from A_3, and coset leader 1 of A_3 in Z_n. Suprisingly, this ordering process for the rows of the ring's table can result in the rows being ordered in the normal counting order of Z_n. In the factorization of Z_n, each of the S_i subrings is a principal ideal, in fact the ideal generated by 2^i. The corresponding A_i is also a principal ideal generated by the smallest element of Z_n which annihilates the generator of S_i, in this case 2^{n-i}. Thus each A_i is the largest subring which will annihilate S_i. This is consistent with our desire to produce a 'fast' matrix as each annihilator element corresponds to an additional strip across the matrix of the basic subblock generated by the product of the subset of representative coset leaders of A_i times the column factoring subring S_i, thereby reducing the size of the subproblems without increasing the number of subproblems.

Notice that all the elements of the additive group of Z_n have a unique representation in terms of the element 1, i.e. k*1. The map $k*1 \mapsto w^k$ gives us a natural homomorphism from the additive group of Z_n to the multiplicative group generated by the principal nth root of unity. Thus our factorization in the ring Z_n is guaranteed to give us a recursive formulation (possibly the usual one) of the actual Fourier matrix. It is

evident from figure 1, that without the mapping being a homomorphism the factorization in the field would not be possible owing to cancellation of multiples of n when computing entries in the ring's multiplication table.

The fast Hadamard transform has a recursive definition of

$$H_n = 1/n \begin{bmatrix} H_{n/2} & H_{n/2} \\ H_{n/2} & -H_{n/2} \end{bmatrix} \qquad H_1 = 1$$

For H_n, where $n = 2^k$, consider the ring $\otimes_k Z_2$ where addition and multiplication are the componentwise operations of Z_2. As before with the fast Fourier transform ring table, we can factor the columns of this ring's table (see figure 2) with a chain of subrings (again ideals), and factor the rows with the corresponding chain of annihilator subrings (ideals). Unlike the fast Fourier transform's Z_n, which can be generated by a single element, $\otimes_k Z_2$ has k independent generators. Picking the k elements which each have a different single nonzero component, not only do we obtain a 'basis' for unique representation of elements in $\otimes_k Z_2$, but the basis elements are orthogonal under multiplication, i.e. pairs of distinct basis elements produce zero when multiplied. For a given S_i, the corresponding A_i is the ideal generated by the one's complement of the componentwise bit pattern of the generator of the S_i ideal. This again gives the largest possible A_i for a given S_i.

Figure 2. Multiplication table factorization of ring $\mathbb{Z}_4\mathbb{Z}_2$ for the discrete Hadamard transform of order 16.

					<7>								8+<7>							
					<3>				4+<3>											
					<1>		2+<1>													
A_1	A_2	A_3	L_3		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
			1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
		2	0	2	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2
			1	3	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
	4	0	0	4	0	0	0	0	4	4	4	4	0	0	0	0	4	4	4	4
			1	5	0	1	0	1	4	5	4	5	0	1	0	1	4	5	4	5
		2	0	6	0	0	2	2	4	4	6	6	0	0	2	2	4	4	6	6
			1	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
8	0	0	0	8	0	0	0	0	0	0	0	0	8	8	8	8	8	8	8	8
			1	9	0	1	0	1	0	1	0	1	8	9	8	9	8	9	8	9
		2	0	10	0	0	2	2	0	0	2	2	8	8	10	10	8	8	10	10
			1	11	0	1	2	3	0	1	2	3	8	9	10	11	8	9	10	11
	4	0	0	12	0	0	0	0	4	4	4	4	8	8	8	8	12	12	12	12
			1	13	0	1	0	1	4	5	4	5	8	9	8	9	12	13	12	13
		2	0	14	0	0	2	2	4	4	6	6	8	8	10	10	12	12	14	14
			1	15	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

where the column subring factorization chain

$$\mathbb{Z}_4\mathbb{Z}_2 \quad S_1 \quad S_2 \quad S_3 \qquad \text{is defined by}$$

$$S_1 = \langle 7 \rangle = \{0,1,2,3,4,5,6,7\}$$

$$S_2 = \langle 3 \rangle = \{0,1,2,3\}$$

$$S_3 = \langle 1 \rangle = \{0,1\}$$

where the row annihilator subring factorization chain

$$\{0\}=A_0 \quad A_1 \quad A_2 \quad A_3 \qquad \text{is defined by}$$

$$A_1 = \langle 8 \rangle = \{0,8\}$$

$$A_2 = \langle 12 \rangle = \{0,4,8,12\}$$

$$A_3 = \langle 14 \rangle = \{0,2,4,6,8,10,12,14\}$$

where L_3 is a set of coset leaders of A_3 in $\mathbb{Z}_4\mathbb{Z}_2$

$$L_3 = \{0,1\}$$

Consider the map f: $\otimes_k Z_2$ |-> field, defined by $(a_1b_1+\ldots+a_kb_k)$ goes to $c_1^{a_1}*\ldots*c_k^{a_k}$, where c_i are arbitrary elements of the field. Since the coset leader of S_i consists of a basis element not occurring in S_i, and the annihilator elements do not share basis elements with their row factoring subsets, we observe from the orthogonality of the basis elements that the map does not have to be a homomorphism to give us a 'fast' factorable recursive matrix in the field.

Chapter II

Factorization of Finite Rings Mapping to Fast Transform Matrices

We have seen examples of the factorization of the row and column entries of the multiplication tables of finite rings which were associated with the well known fast Fourier transform and fast Hadamard transforms. We would like to examine sufficient conditions involving the ring's factorization and an 'exponential' map to a field which will guarantee factorization and fast multiplication of the field matrix times a column vector. As motivated by the previous examples, a more general form of a ring's factorization for a single stage is depicted in figure 3.

Representation and the Exponential Map

First we should consider the mechanism for translating the factored ring table into a matrix of elements of the field. This depends on an 'exponential' map from the ring to the field. In order to represent elements of the ring we pick a minimal additive generating set of elements of the ring, $\{b_1,\ldots,b_k\}$. We use this set as a 'basis' for the ring so as to establish a unique representation of each element in the ring, i.e. $r = n_1b_1+\ldots+n_kb_k$ where the n_i are integers.

The 'exponential' map is a mapping $f:R\to F$, which takes each basis element b_i of the ring to an element w_i of the field, i.e. $b_i \mapsto w_i$, so that a linear combination of the basis elements is carried to a product of powers of

Figure 3. One stage of the factorization of a ring's multiplication table. The set $S_i=\{S_j\}$ is the column factoring subring. The g_j are representative coset leaders of S_i factoring S_{i-1}. The a_j's belong to A_i, the row factoring annihilator ring. $L_i=\{l_j\}$ is a representative set of coset leaders of A_i factoring A_{i+1}.

	$g_1 + S_i$	$g_2 + S_i$	...	$g_j + S_i$
l_1				
.				
$a_1 + .$	$(a_1+L_i)*(g_1+S_i)$	$a_1g_2+L_ig_2+L_iS_i+a_1S_i$	...	$(a_1g_j+L_i)*(g_j+S_i)$
.				
l_k				
l_1		$a_2g_2+l_1g_2+l_1S_i+a_2S_i$		
l_2		$a_2g_2+l_2g_2+l_2S_i+a_2S_i$		
$a_2 + .$	$(a_2+L_i)*(g_1+S_i)$	.	...	$(a_2g_j+L_i)*(g_j+S_i)$
.		.		
l_k		$a_2g_2+l_kg_2+l_kS_i+a_2S_i$		
.				
.				
.				
l_1				
.				
$a_m + .$	$(a_m+L_i)*(g_3+S_i)$	$a_mg_2+L_ig_2+L_iS_i+a_mS_i$	...	$(a_mg_j+L_i)*(g_j+S_i)$
.				
l_k				

the w_i, i.e. $(n_1b_1+\ldots+n_kb_k) \mapsto w_1^{n_1}*\ldots*w_k^{n_k}$. Given a factorization of the row and column entries of the ring's multiplication table, entries within the table will be derived from the product of the factored row and column elements of the table, i.e. $(a_i+l_k)*(g_j+s_m) = a_i*g_j + l_k*g_j + a_i*s_m + l_k*s_m$, (see figure 3) where a_i is an annihilator element, l_k is an element of the row 'representative leaders' factor set, g_j is a column decomposition coset leader, and s_m is an element of the column factoring subring. Note that if the map f is a homomorphism then we are guaranteed that the sum of the four addends in the ring will map over to the field as though the map was being applied to each addend independently, i.e. f(a+b+c+d) = f(a)*f(b)*f(c)*f(d), producing a product of four factors in the field, thus allowing the successful factorization of subblocks of a stage into four matrix products as depicted in figure 4. If f is a homomorphism, then since R is a finite ring all the basis elements b_i have finite order implying that the w^i are roots of unity, i.e. $n_i*b_i = 0$ for some n_i, so that $f(n_i*b_i) = f(0) = w_i^{n_i} = 1$. If f is not a homomorphism, then we face possible cancellation of sums of basis elements in the expressions producing entries in the ring's multiplication table, which will then possibly produce missing factors in the field matrix produced by the mapping f.

The homomorphism requirement becomes unnecessary if

1) the 'basis' elements of the ring are orthogonal under multiplication, i.e. the multiplication of any two distinct basis elements produces zero.
2) the column coset leaders do not share any basis elements with the elements of the column factoring subset,
3) the annihilator elements share no basis elements with the subset of representative leaders which factor the rows, and
4) the annihilating elements a_i in fact do take all the elements s_m of the column factoring subring to zero under multiplication.

This way the three remaining possibly nonzero elements of the ring entry sum have no basis elements in common. Thus when mapped to the field F by an exponential map, the three remaining addends make an independent contribution to the product without the necessity of a homomorphism to cope with possible cancellation in the ring when sums of the 'basis' elements are taken. This allows the w_i's to be arbitrary, even 0. These four requirements are met by the $\otimes_k Z_2$ example ring given for the Hadamard transform.

Row and Column Factoring with its Implication for Complexity

In our previous examples, the column entries of the multiplication table were factored by an ideal. The columns could be factored just as well by a subring considering the factorization as that of an additive group. It is even possible that the columns could be

additively factored by a mere subset. In our previous examples the rows were factored in an 'inverted' coset fashion, with the actual annihilator ideal (only necessarilly a subring) elements acting as 'leaders', and a set of the representative coset leaders of the annihilator subring factorization acting as the factoring subset. Let us consider whether it is necessary for the 'annihilator' elements to take all the elements of the column factoring subset to zero. Observe in figure 4 the translation of one subblock of the ring's table into its corresponding matrix product representation in the field produced by the given exponential map. Observe in figure 5a that the product of these four matrices will multiply subvector V_j of the column vector V. Submatrix X is the basic computational unit common to all the subblocks. If matrix T_k is not a scalar matrix (constant times the identity matrix), but rather a diagonal matrix as written in figure 4, this forces the product of X times a vector to be done in all j*j possible cases assuming both the rows and columns factor into j pieces, (unequal splits are mentioned in later sections on Nonsingularity, Speedup, and the corresponding recurrence relation is developed and solved in the Appendix), resulting in a needlessly complicated recursive $O(n^2)$ multiplication algorithm. Observe figure 5a to see the necessity of all these products as although the T_k are the same across each row of subblocks, the T_k are different for different rows,

Figure 4. $\text{Subblock}_{2,3}$ of stage i of the ring factorization

$$(a_2+L_i)*(g_3+S_i) = (a_2*g_3)+(L_i*g_3)+(L_i*S_i)+(a_2*S_i) = \begin{bmatrix} a_2g_3+l_1g_3+l_1S_i+a_2S_i \\ a_2g_3+l_2g_3+l_2S_i+a_2S_i \\ \vdots \\ a_2g_3+l_kg_3+l_kS_i+a_2S_i \end{bmatrix}$$

Maps to the field as:

$$\begin{bmatrix} f(a_2g_3)*f(l_1g_3)*f(l_1s_1)*f(a_2s_1) & \dots & f(a_2g_3)*f(l_1g_3)*f(l_1s_p)*f(a_2s_p) \\ f(a_2g_3)*f(l_2g_3)*f(l_2s_1)*f(a_2s_1) & \dots & f(a_2g_3)*f(l_2g_3)*f(l_2s_p)*f(a_2s_p) \\ \vdots & & \vdots \\ f(a_2g_3)*f(l_kg_3)*f(l_ks_1)*f(a_2s_1) & \dots & f(a_2g_3)*f(l_kg_3)*f(l_ks_p)*f(a_2s_p) \end{bmatrix}$$

Factors in the field as:

$$\begin{bmatrix} f(a_2g_3) & & \\ & \ddots & 0 \\ 0 & & f(a_2g_3) \end{bmatrix} * \begin{bmatrix} f(l_1g_3) & & \\ & \ddots & 0 \\ 0 & & f(l_kg_3) \end{bmatrix} * \begin{bmatrix} f(l_1s_1) & \dots & f(l_1s_m) \\ \vdots & & \vdots \\ f(l_ks_1 & \dots & f(l_ks_m) \end{bmatrix} * \begin{bmatrix} f(a_2s_1) & & \\ & \ddots & 0 \\ 0 & & f(a_2s_k) \end{bmatrix}$$

C_{23} D_3 X T_2

Figure 5a. General form of field matrix resulting from the mapping of one stage of a ring's multiplication table (with notation as in text) shown multiplying a column vector.

$$\begin{bmatrix} C_{11}D_1XT_1 & C_{12}D_2XT_1 & C_{13}D_3XT_1 & \cdots & C_{1n}D_nXT_1 \\ C_{21}D_1XT_2 & C_{22}D_2XT_2 & C_{23}D_3XT_2 & \cdots & C_{2n}D_nXT_2 \\ C_{31}D_1XT_3 & C_{32}D_2XT_3 & C_{33}D_3XT_3 & \cdots & C_{3n}D_nXT_3 \\ C_{41}D_1XT_4 & C_{42}D_2XT_4 & C_{43}D_3XT_4 & \cdots & C_{4n}D_nXT_4 \\ \vdots & \vdots & \vdots & & \vdots \\ C_{m1}D_1XT_m & C_{m2}D_2XT_m & C_{m3}D_3XT_m & \cdots & C_{mn}D_nXT_m \end{bmatrix} \begin{bmatrix} V_1 \\ V_2 \\ V_3 \\ V_4 \\ \vdots \\ V_n \end{bmatrix}$$

Figure 5b. Assuming the T_j are scalar matrices, they commute with D_iX and can be combined with the C_{ij} scalar matrices to form the following matrix where c_{ij} is a scalar constant.

$$\begin{bmatrix} c_{11}D_1X & c_{12}D_2X & c_{13}D_3X & \cdots & c_{1n}D_nX \\ c_{21}D_1X & c_{22}D_2X & c_{23}D_3X & \cdots & c_{2n}D_nX \\ c_{31}D_1X & c_{32}D_2X & c_{33}D_3X & \cdots & c_{3n}D_nX \\ c_{41}D_1X & c_{42}D_2X & c_{43}D_3X & \cdots & c_{4n}D_nX \\ \vdots & \vdots & \vdots & & \vdots \\ c_{m1}D_1X & c_{m2}D_2X & c_{m3}D_3X & \cdots & c_{mn}D_nX \end{bmatrix} \begin{bmatrix} V_1 \\ V_2 \\ V_3 \\ V_4 \\ \vdots \\ V_n \end{bmatrix}$$

Figure 5c. The matrix product in 5b can be rewritten as

$$\begin{bmatrix} c_{11} & c_{12} & c_{13} & \cdots & c_{1n} \\ c_{21} & c_{22} & c_{23} & \cdots & c_{2n} \\ c_{31} & c_{32} & c_{33} & \cdots & c_{3n} \\ c_{41} & c_{42} & c_{43} & \cdots & c_{4n} \\ \vdots & \vdots & \vdots & & \vdots \\ c_{m1} & c_{m2} & c_{m3} & \cdots & c_{mn} \end{bmatrix} \begin{bmatrix} D_1XV_1 \\ D_2XV_2 \\ D_3XV_3 \\ D_4XV_4 \\ \vdots \\ D_nXV_n \end{bmatrix}$$

meaning that for all subblocks X will be multiplying possibly distinct vectors. However if the matrix T_k is scalar, then T_k will commute with matrix X so that the four matrix product becomes $C_{rc}D_jT_kX$. If all the T_k are scalar, then the product of X times the V_j need only occur once for each of the j subvectors V_j. To finish the product evaluation for each subblock it is only necessary to multiply the appropriate $X*V_j$ by the diagonal matrix product $C_{rc}D_jT_k$ which requires n/j multiplications, where n is the number of columns in this stage. Since there are j*(j-1) subblocks requiring multiplication by the $C_{rc}D_jT_k$ diagonal matrices (all but the first column of subblocks), we have j*(j-1)*n/j = (j-1)*n additional multiplications to perform after the computation of the j distinct $X*V_j$ matrix times vector subproblems, in order to complete the computation for one stage. For counting the number of additions, recursively we have j size n/j subproblems, which when combined to produce an answer require j summations (one for each of the j row splits) of j vectors (one for each of the j column splits) of length n/j costing j*((j-1)*n/j) = (j-1)*n additions. Thus the same number of additions are required as multiplications. Recursively applying this process to X and its descendents leads us to the following recurrence relation for the count of multiplications or additions (assuming for simplicity each stage splits rows and columns into j pieces) : T(n) = j*T(n/j) + (j-1)*n, which has an O(nlogn)

solution.

The matrix T_k in the four matrix field product of figure 4 is derived from the product of an 'annihilator' element times the elements of the column factoring subset. Since the product $a_i * s_m$, 'annihilator' element a_i times the elements s_m of the column factoring subring (or subset), is the same for each column of the subblock we deduce that the matrix T_k postmultiplies basic subblock matrix X in this product. If a_i is a genuine annihilator of all the elements of S_i, then the map to the field will result in the T_k matrix being the identity matrix. For T_k to be a scalar matrix, all that is necessary is that each 'annihilator' element 'levels' the elements of S_i, i.e. takes all the elements of S_i to the same constant, possibly a different constant for each annihilator element of A_i. If S_i is a subring or else a subset containing the element zero, then necessarily the constant will be zero and the 'annihilator' elements will be true annihilators. The set of elements $\{a_i\}$ taking S_i to some constant, possibly a different constant for each element a_i, does form a subring since it is closed under addition and multiplication and contains the element zero. We shall see that we want to use the whole annihilator subring for factoring, rather than a subset, to maximize speedup and also to prevent singularity of the resulting field matrix.

We have seen that possibly the column factoring subrings S_i could be subsets and the row 'annihilator'

elements need only 'level' or take the elements in S_i to a constant, i.e. $\{a_i * S_i\} = \{c_i\}$.

Suppose we are given a chain of subsets which factor R, $R=S_0 \supset S_1 \supset S_2 \supset \ldots \supset S_k$, where each S_{i+1} is a maximal factoring subset of S_i, (maximal factoring subset means that no set S properly containing S_{i+1} is a factoring subset of S_i). Correspondingly, we will require a chain of distinct subrings $\{0\} \subset A_1 \subset A_2 \subset \ldots \subset A_k$, which are maximal and 'level' their corresponding S_i's. We would like to show that given the above conditions, without loss of generality we may as well consider the S_i's to be subrings and hence the A_i's true annihilator subrings. Pick an arbitrary element s_j from S_k. Form the chain $R=S_0-\{s_j\} \supset S_1-\{s_j\} \supset S_2-\{s_j\} \supset \ldots \supset S_k-\{s_j\}$. The element zero is a member of every subset of the chain. Notice that the chain of 'leveller' subrings are true annihilator subrings for the new chain of column factoring subsets, i.e. $a*(s-s_j)=c-c=0$ for $a \in A_i$, $s \in S_i$. Now, take the additive and multiplicative closure of each of the new subsets so as to obtain the chain $R=\bar{S}_0 \supset \bar{S}_1 \supset \bar{S}_2 \supset \ldots \supset \bar{S}_k$ of subrings. Notice the chain of $\{0\} \subset A_1 \subset A_2 \subset \ldots \subset A_k$ still annihilate the corresponding $\bar{S}_i$. Since we have assumed that S_{i+1} factoring S_i was maximal, starting with i=0, increment i comparing the ratio of $|S_i/S_{i+1}|$ with $|S_i/S_{i+1}|$ until either i reaches k-1 or until the ratios are different, i.e. $|\bar{S}_i/\bar{S}_{i+1}|$ is smaller. If i reaches k-1, then the chain $R \supset S_1-\{s_j\} \supset \ldots \supset S_k-\{s_j\}$ is a maximal

chain of subrings factoring the columns, since $S_i \subset \bar{S}_i$ and $|S_i| = |\bar{S}_i|$. If a different ratio is reached before i reaches k-1, then create the chain $R=S_0 \supset \bar{S}_1+\{s_j\} \supset \ldots \supset \bar{S}_k+\{s_j\}$. This chain is identical with the original chain through position i. We have $S_{i+1} \subset \bar{S}_{i+1}+\{s_j\}$ and $|S_{i+1}| < |\bar{S}_{i+1}+\{s_j\}|$, since S_{i+1} was assumed a maximal factoring subset of S_i, we have arrived at a contradiction. So there must not have been an i which gave us different ratios, implying the chain of maximal subsets was at worst a chain of cosets of a chain of subrings, easily translatable to a chain of subrings. Notice also that if two $S_m-\{s_j\}$ and $S_n-\{s_j\}$ for $m<n$ generate the same subring we could not have had A_m and A_n maximal and distinct for levelling S_m and S_n since both A_m and A_n annihilate this same subring.

Therefore, without loss of generality we might as well consider the chain $R=S_0 \supset S_1 \supset S_2 \supset \ldots \supset S_k$ to be a chain of maximal subrings, and the chain $\{0\}=A_0 \subset A_1 \subset A_2 \subset \ldots \subset A_k$ to be a chain of maximal true annihilator subrings of the corresponding S_i's. From later observations on speedup and orthogonality of the field matrix, we prefer or need the maximality of both chains.

Nonsingularity of the Field Matrix

Given the factorization of the ring's multiplication table, we want to know under what conditions the resultant matrix in the field will be nonsingular. Recursively, if we consider the matrix product of the entire block of one

stage of the factorization times its portion of the column vector (see figure 5b), we observe that

1) if the basic subblock X is singular, then so is the whole block and the whole matrix,
2) if any of the diagonal matrices $D_1, D_2, \ldots$ are singular then it is possible to pick a nonzero column vector which is taken to zero, so that again the matrix is singular.
3) if the matrix of the field elements corresponding to the product of the row annihilator and column coset leader for each subblock (see figure 5c) is nonsingular and the diagonal D_j's and the basic subblock X are nonsingular, then the whole block is nonsingular. This follows since figure 5b is equivalent to figure 5c where $(D_jX)*V_j$ are effectively arbitrary vectors because of the nonsingularity of (D_jX).
4) If at any stage of the factorization the rows split into more subblocks than the columns, then we can create a zero row as a linear combination of the rows corresponding to the same row factoring subset element. See figure 6 for an example. Thus if we desire a nonsingular field matrix then we must have the ratio of $|A_{i+1}/A_i| <= |S_i/S_{i+1}|$.
5) If an annihilator element exists for an S_i, but is not contained in A_i, then for that stage there will exist a linear combination of the rows associated

Figure 6. Singularity of the field matrix will result if the ring factors into more row sets than column sets for any stage.

$$\begin{bmatrix} X & c_{12}D_2X & c_{13}D_3X \\ X & c_{22}D_2X & c_{23}D_3X \\ X & c_{32}D_2X & c_{33}D_3X \\ X & c_{42}D_2X & c_{43}D_4X \end{bmatrix} \begin{bmatrix} V_1 \\ V_2 \\ V_3 \end{bmatrix}$$

Since the above matrix product is equivalent to

$$\begin{bmatrix} 1 & c_{12} & c_{13} \\ 1 & c_{22} & c_{23} \\ 1 & c_{32} & c_{33} \\ 1 & c_{42} & c_{43} \end{bmatrix} \begin{bmatrix} D_1XV_1 \\ D_2XV_2 \\ D_3XV_3 \end{bmatrix}$$

This matrix is clearly singular, i.e. a zero row can be produced by simple row elimination.

with this element in the row factor sets which will sum to zero, hence causing singularity. This follows easily from having one more row available than the number of scalar multiples of identical subsegments contained in the rows, with a zero row being produced in a similar fashion as the elimination in figure 6.

Speedup

Since more row factors than column factors in the ring factorization leads to singularity in the field's matrix, we are left with either an equal number of row and column factors or else more column factors than row factors as possibilities. Equal numbers of row and column factors leads to the recurrence relation $T(n) = j*T(n/j) + (j-1)*n$ for the number of operations, which has an $O(n\log n)$ solution. Having more column factors than row factors leads to a two variable recurrence relation for the operation count, $T(n,m) = j*T(n/k,m/j) + k*m*(j-1)/j$ where n is the number of rows, n the number of columns, k the number of row splits, and j the number of column splits, which still has an $O(n\log n)$ solution (developed and solved in the appendix). Even if at each stage we have a different ratio of column factors to row factors, we can bound the operation count by the largest ratio to find that the operation count for the ring factorization approach is bounded by $O(n\log n)$.

Summary

Given a matrix M of elements from a field F, there

exists a 'fast' multiplication of M times a column vector V if there exists a finite ring R satisfying the following requirements:

1) the elements of R can be uniquely represented in terms of a minimal additive generating set $\{b_1,\ldots,b_k\}$ which acts like a basis, i.e. for every r in R there exists a unique linear combination of the b_i such that $r = n_1b_1+\ldots+n_kb_k$.
2) there exists a chain of distinct subrings $R=S_0 \supset S_1 \supset \ldots \supset S_k$ where S_{i+1} is maximal factoring S_i, i.e. no larger $S \supset S_{i+1}$ factors S_i. Note: the weaker assumption that the S_i are just subsets leads to the conclusion that the S_i are either subrings or cosets of subrings. Correspondingly there is a chain of distinct maximal annihilator subrings $\{0\} \subset A_1 \subset A_2 \subset \ldots \subset A_k$, for which the product $A_i*S_i=\{0\}$ and the product $A_j*S_i=\{0\}$ for $j>i$.
3) R and F are related by an exponential map $f:R\to F$, such that the range of f is the set {elements of M}, defined on the generators of R by $f(n*b_i)=w_i^{\,n}$.
   a) if f is a homomorphism then we have
      $f(n_1*b_1+\ldots+n_k*b_k) = w_1^{\,n_1}*\ldots*w_k^{\,n_1}$
      which guarantees proper factorization in the field matrix. Notice the w's have to be roots of unity.
   b) if 1) the 'basis' elements are multiplicatively orthogonal, 2) if the basis elements used to represent the column coset leaders for each stage

do not occur in any of the elements of their respective column factoring rings, and 3) the same holds for the annihilator elements and their corresponding factoring leader subsets, then we also are guaranteed factorization in the matrix M without requiring a homomorphism. This eliminates the need for the w's to be roots of unity.

Possibilities other than strictly a) or b) exist to guarantee the proper factorization of the field matrix M. Take the direct product of a ring which is factorable from being orthogonal and another which has a homomorphism, giving us a ring (with operations defined in componentwise fashion) which satisfies neither of the two mentioned sufficient conditions, but which maps to a factorable matrix in the field. This map is defined in componentwise fashion using the appropriate maps for each constituent ring.

4) one necessary requirement for nonsingularity is that the number of row splits not exceed the number of column splits for any stage.

The decomposition of one stage of the factorization occurs as in figure 1 for the ring and figure 5 for the matrix produced by the mapping to the field.

Chapter III

Examples of Factorable Finite Rings Producing Factorable Field Matrices

Fast Fourier transform matrices of composite order and the Kronecker products (see appendix) of the matrices of Fourier transforms of various orders can easily be described by ring factorizations. Consider the Fourier transform of composite order twelve associated with the ring Z_{12}. According to our requirement of picking a maximal column factor group at each stage we can arrive at the factorization in figure 7a. This factorization produces a field matrix which when multiplied times a column vector requires 60 multiplications. If instead we factor the ring as in figure 7b with a different maximal chain, again we find that 60 multiplications are required. Let us consider a similar but larger example, again counting the number of operations for different but maximal factorizations.

Consider the Fourier transform of order 24, with column factorization chain $Z_{24} \supset \langle 2 \rangle \supset \langle 4 \rangle \supset \langle 8 \rangle$ with annihilator chain $\{0\} \subset \langle 12 \rangle \subset \langle 6 \rangle \subset \langle 3 \rangle$. We compute the number of operations from the recurrence T(n)=j*T(n/j) + (j-1)*n, where the number of row and column splits happens to be the same, i.e. equals j, for a particular stage.

T(3) = 9
T(6) = 2*T(3) + 6 = 18 + 6 = 24
T(12) = 2*T(6) + 12 = 48 + 12 = 60
T(24) = 2*T(12) + 24 = 120 + 24 = 144

Figure 7a. Factorization of Z_{12} with
column factorization Z_{12} <3> <6>
annihilator factorization {0} <4> <2>

				<3>				1+<3>				2+<3>			
				<6>		3+<6>									
A_1	A_2	L		0	6	3	9	1	7	4	10	2	8	5	11
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
		1	1	0	6	3	9	1	7	4	10	2	8	5	11
	2	0	2	0	0	6	6	2	2	8	8	4	4	10	10
		1	3	0	6	9	3	0	9	0	6	0	0	3	9
4	0	0	4	0	0	0	0	4	4	4	4	8	8	8	8
		1	5	0	6	3	9	4	10	7	1	8	2	11	5
	2	0	6	0	0	6	6	4	4	10	10	8	8	2	2
		1	7	0	6	9	3	4	10	1	7	8	2	5	11
8	0	0	8	0	0	0	0	8	8	8	8	4	4	4	4
		1	9	0	6	3	9	8	2	11	5	4	10	7	1
	2	0	10	0	0	6	6	8	8	2	2	4	4	10	10
		1	11	0	6	9	3	8	2	5	11	4	10	1	7

Figure 7b. Factorization of Z_{12} with
column chain Z_{12} <2> <4>
annihilator chain {0} <6> <3>

				<2>						1 + <2>					
				<4>			2+<4>								
A_1	A_2	L		0	4	8	2	6	10	1	5	9	3	7	11
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
		1	1	0	4	8	2	6	10	1	5	9	3	7	11
		2	2	0	8	4	4	0	8	1	9	5	5	1	9
	3	0	3	0	0	0	6	6	6	3	3	3	9	9	9
		1	4	0	4	8	8	0	4	4	8	0	0	4	8
		2	5	0	8	4	10	6	2	0	13	9	3	11	7
6	0	0	6	0	0	0	0	0	0	6	6	6	6	6	6
		1	7	0	4	8	2	6	10	7	11	3	9	1	5
		2	8	0	8	4	4	0	8	0	4	0	0	8	4
	3	0	9	0	0	0	6	6	6	9	9	9	3	3	3
		1	10	0	4	8	8	0	4	10	2	6	6	10	2
		2	11	0	8	4	10	6	2	11	7	3	9	5	1

If we factor the ring with a different maximal chain as $Z_{24} \supset \langle 3 \rangle \supset \langle 6 \rangle \supset \langle 12 \rangle$ with annihilator chain $\{0\} \subset \langle 8 \rangle \subset \langle 4 \rangle \subset \langle 2 \rangle$, then we get the following operation count.

$T(2) = 4$
$T(4) = 2*T(2) + 4 = 12$
$T(8) = 2*T(4) + 8 = 32$
$T(24) = 3*T(8) + 2*24 = 96 + 48 = 144$

The number of multiplications (and additions) is the same in both factorizations, so that at least in these two cases maximal factorizations lead to equally fast computations.

The ring $Z_n \otimes Z_m$ can correspond to the Kronecker product of the Fourier matrices F_n and F_m. See figure 8 for factorizations of $Z_3 \otimes Z_4$ leading to both $F_3 \otimes F_4$ and $F_4 \otimes F_3$. In general, we can form $\otimes_j Z_{k_i}$ which can be mapped to a sequence of j Kronecker products of the submatrices F_{k_i} in any order. Note that the Kronecker product of a string of Fourier matrices F_{k_i} is not commutative, whereas the ring $\otimes_j Z_{k_i}$ can be interpreted as the Kronecker product of the matrices F_{k_i} in any order. This indicates a structural variety of matrices which can be produced from this ring, although the structures have the same flavor.

Finite polynomial rings are an easy source of examples, in fact the Z_n Fourier rings are trivially $Z_n[x]$ mod x. A less trivial example is $Z_2[x]$ mod x^4+1. One factorization for this ring is shown in figure 9. The column factorization can be done with a chain of ideals $R \supset \langle x+1 \rangle \supset \langle (x+1)^2 \rangle \supset \langle (x+1)^3 \rangle$ with the corresponding

Figure 8. Factorization of $Z_3 \oplus Z_4$

Giving $F_4 \oplus F_3$

A_1	A_2	L		$z_3 0+00$			$z_3 0+02$			$z_3 0+01$			$z_3 0+03$		
				00	10	20	02	12	22	01	11	21	03	13	23
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
		10	10	00	10	20	00	10	20	00	10	20	00	10	20
		20	20	00	20	10	00	20	10	00	20	10	00	20	10
	01	00	01	00	00	00	02	02	02	01	01	01	03	03	03
		10	11	00	10	20	02	12	22	01	11	21	03	13	23
		20	21	00	20	10	02	22	12	01	21	11	03	23	13
02		00	02	00	00	00	00	00	00	02	02	02	02	02	02
		10	12	00	10	20	00	10	20	02	12	22	02	12	22
		20	22	00	20	10	00	20	10	02	22	12	02	22	12
	01	00	03	00	00	00	02	02	02	02	02	02	00	00	00
		10	13	00	10	20	02	12	22	02	12	22	00	10	20
		20	23	00	20	10	02	22	12	02	22	12	00	20	10

Giving $F_3 \oplus F_4$

A_1	L		$0z_4+00$				$0z_4+10$				$0z_4+20$			
			00	02	01	03	10	12	11	13	20	22	21	23
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	01	01	00	02	01	03	00	02	01	03	00	02	01	03
	02	02	00	00	02	02	00	00	02	02	00	00	02	02
	03	03	00	02	03	01	00	02	03	01	00	02	03	01
10	00	10	00	00	00	00	10	10	10	10	20	20	20	20
	01	11	00	02	01	03	10	12	11	13	20	22	21	23
	02	12	00	00	02	02	10	10	12	12	20	20	22	22
	03	13	00	02	03	01	10	12	13	11	20	22	23	21
20	00	20	00	00	00	00	20	20	20	20	10	10	10	10
	01	21	00	02	01	03	20	22	21	23	10	12	11	13
	02	22	00	00	02	02	20	20	22	22	10	10	12	12
	03	23	00	02	03	01	20	22	23	21	10	12	13	11

Notational example: $z_3 0+02 = \{ \langle 0,0\rangle+\langle 0,2\rangle, \langle 1,0\rangle+\langle 0,2\rangle, \langle 2,0\rangle+\langle 0,2\rangle \}$

$= \{ \langle 0,2\rangle, \langle 1,2\rangle, \langle 2,2\rangle \}$

Figure 9. Factorization of $Z_2[x]$ mod x^4+1

						$\langle x+1\rangle$								$1+\langle x+1\rangle$							
						$\langle(x+1)^2\rangle$					$(x+1)+\langle(x+1)^2\rangle$										
						$\langle(x+1)^3\rangle$		$(x^2+1)+\langle(x+1)^3\rangle$													
A1	A2	A3	L			0	x^3+x^2+x+1	x^2+1	x^3+3	$x+1$	x^3+x^2	x^2+x	x^3+1	1	x^3+x^2+x	x^2	x^3+x+1	x	x^3+x^2+1	x^2+x+1	x^3
0	0	0	0	0	;	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
			1	1	;	0	x^3+x^2+x+1	x^2+1	x^3+x	$x+1$	x^3+x^2	x^2+x	x^3+1	1	x^3+x^2+x	x^2	x^3+x+1	x	x^3+x^2+1	x^2+x+1	x^3
		$(x+1)$	0	$x+1$	;	0	0	x^3+x^2+x+1	x^3+x^2+x+1	x^2+1	x^2+1	x^3+x	x^3+x	$x+1$	$x+1$	x^3+x^2	x^3+x^2	x^2+x	x^2+x	x^3+1	x^3+1
			1	x	;	0	x^3+x^2+x+1	x^3+x	x^2+1	x^2+x	x^3+1	x^3+x^2	$x+1$	x	x^3+x^2+1	x^3	x^2+x+1	x^2	x^3+x+1	x^3+x^2+x	1
	$(x+1)^2$	0	0	x^2+1	;	0	0	0	0	x^3+x^2+x+1	x^3+x^2+x+1	x^3+x^2+x+1	x^3+x^2+x+1	x^2+1	x^2+1	x^2+1	x^2+1	x^3+x	x^3+x	x^3+x	x^3+x
			1	x^2	;	0	x^3+x^2+x+1	x^2+1	x^3+x	x^3+x^2	$x+1$	x^3+1	x^2+x	x^2	x^3+x+1	1	x^3+x^2+x	x^3	x^2+x+1	x^3+x^2+1	x
		$(x+1)$	0	x^2+x	;	0	0	x^3+x^2+x+1	x^3+x^2+x+1	x^3+x	x^3+x	x^2+1	x^2+1	x^2+x	x^2+x	x^3+1	x^3+1	x^3+x^2	x^3+x^2	$x+1$	$x+1$
			1	x^2+x+1	;	0	x^3+x^2+x+1	x^3+x	x^2+1	x^3+1	x^2+x	$x+1$	x^3+x^2	x^2+x+1	x^3	x^3+x^2+1	x	x^3+x^2+x	1	x^2	x^3+x+1
$(x+1)^3$	0	0	0	x^3+x^2+x+1	;	0	0	0	0	0	0	0	x^3+x^2+x+1	x^3+x^2+x+1	x^3+x^2+x+1	x^3+x^2+x+1	x^3+x^2+x+1	x^3+x^2+x+1	x^3+x^2+x+1	x^3+x^2+x+1	x^3+x^2+x+1
			1	x^3+x^2+x	;	0	x^3+x^2+x+1	x^2+1	x^3+x	$x+1$	x^3+x^2	x^2+x	x^3+1	x^3+x^2+x	1	x^3+x+1	x^2	x^3+x^2+1	x	x^3	x^2+x+1
		$(x+1)$	0	x^3+x^2	;	0	0	x^3+x^2+x+1	x^3+x^2+x+1	x^2+1	x^2+1	x^3+x	x^3+x	x^3+x^2	x^3+x^2	$x+1$	$x+1$	x^3+1	x^3+1	x^2+x	x^2+x
			1	x^3+x^2+1	;	0	x^3+x^2+x+1	x^3+x	x^2+1	x^2+x	x^3+1	x^3+x^2	$x+1$	x^3+x^2+1	x	x^2+x+1	x^3	x^3+x+1	x^2	1	x^3+x^2+x
	$(x+1)^3$	0	0	x^3+x	;	0	0	0	0	x^3+x^2+x+1	x^3+x^2+x+1	x^3+x^2+x+1	x^3+x^2+x+1	x^3+x	x^3+x	x^3+x	x^3+x	x^2+1	x^2+1	x^2+1	x^2+1
			1	x^3+x+1	;	0	x^3+x^2+x+1	x^2+1	x^3+x	x^3+x^2	$x+1$	x^3+1	x^2+x	x^3+x+1	x^2	x^3+x^2+x	1	x^2+x+1	x^3	x	x^3+x^2+1
		$(x+1)$	0	x^3+1	;	0	0	x^3+x^2+x+1	x^3+x^2+x+1	x^3+x	x^3+x	x^2+1	x^2+1	x^3+1	x^3+1	x^2+x	x^2+x	$x+1$	$x+1$	x^3+x^2	x^3+x^2
			1	x^3	;	0	x^3+x^2+x+1	x^3+x	x^2+1	x^3+1	x^2+x	$x+1$	x^3+x^2	x^3	x^2+x+1	x	x^3+x^2+1	1	x^3+x^2+x	x^3+x+1	x^2

annihilator chain $\{0\} \subset \langle (x+1)^3 \rangle \subset \langle (x+1)^2 \rangle \subset \langle (x+1) \rangle$. We have numerous alternatives for a basis set, for example $\{1, x, x^2, x^3\}$ or possibly $\{(x+1)^3, (x+1)^2, (x+1), 1\}$. If the exponential map carries the basis elements into the second roots of unity, 1 and -1, then the exponential map will be a homomorphism thus guaranteeing factorization of the field transform matrix. Hadamard matrix, e.g. map the basis elements $(x+1)^2$, $(x+1)$, and 1 of the ring to the element 1 of the field, and map $(x+1)^3$ to the element -1 of the field.

Another example of a polynomial ring is $Z_4[x]$ mod x^2+1. In this case (figure 10), the column subring factorization can be done with $R \supset \langle x+1 \rangle \supset \langle 2 \rangle \supset \langle 2x+2 \rangle$. The annihilator factorization is again a chain of ideals $\{0\} \subset \langle 2x+2 \rangle \subset \langle 2 \rangle \subset \langle x+1 \rangle$. A minimal additive generating set is $\{1, x+1\}$. Although there are only two basis elements, we could choose to represent the set of elements generated by a single basis element in a 'radix' notation, using a multiple of a basis element as a place holder. We could choose to represent elements of this ring uniquely in terms of $\{1, 2, x+1, 2x+2\}$. This would require relations on the elements of the field F such that

$w_1 * w_1 = f(1) * f(1) = f(2) = w_2$ and

$w_3 * w_3 = f(x+1) * f(x+1) = f(2x+2) = w_4$, with $w_2 * w_2 = 1$, $w_4 * w_4 = 1$.

This would suffice to give us a homomorphism providing factorization, as no orthogonal basis with four elements is available here. This ring will not map into a Hadamard

Figure 10. Factorization of $Z_4[x]$ mod x^2+1

						<2x+2>		2+<2x+2>		<x+1>		(x+1) + <2>		<2>		1 + <x+1>							
A_1	A_2	A_3	L			0	2x+1	2	2x	x+1	3x+3	x+3	3x+1	1	2x+3	3	2x+1	x+2	3x	x	3x+2
0	0	0	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
			1	1		0	2x+2	2	2x	x+1	3x+3	x+3	3x+1	1	2x+3	3	2x+1	x+2	3x	x	3x+2
		x+1	0	x+1		0	0	2x+2	2x+2	2x	2x	2	2	x+1	x+1	3x+3	3x+3	3x+1	3x+1	x+3	x+3
			1	x+2		0	2x+2	2x	2	3x+1	x+3	x+1	3x+3	x+2	3x	3x+2	x	3	2x+1	2x+3	1
	2	0	0	2		0	0	0	0	2x+2	2x+2	2x+2	2x+2	2	2	2	2	2x	2x	2x	2x
			1	3		0	2x+2	2	2x	3x+3	x+1	3x+1	x+3	3	2x+1	1	2x+3	3x+2	x	3x	x+2
		x+1	0	x+3		0	0	2x+2	2x+2	2	2	2x	2x	x+3	x+3	3x+1	3x+1	x+1	x+1	3x+3	3x+3
			1	x		0	2x+2	2x	2	x+3	3x+1	3x+3	x+1	x	3x+2	3x	x+2	2x+3	1	3	2x+1
2x+2	0	0	0	2x+2		0	0	0	0	0	0	0	0	2x+2	2x+2	2x+2	2x+2	2x+2	2x+2	2x+2	2x+2
			1	2x+3		0	2x+2	2	2x	x+1	3x+3	x+3	3x+1	2x+3	1	2x+1	3	3x	x+2	3x+2	x
		x+1	0	3x+3		0	0	2x+2	2x+2	2x	2x	2	2	3x+3	3x+3	x+1	x+1	x+3	x+3	3x+1	3x+1
			1	3x		0	2x+2	2x	2	3x+1	x+3	x+1	3x+3	3x	x+2	x	3x+2	2x+1	3	1	2x+3
	2	0	0	2x		0	0	0	0	2x+2	2x+2	2x+2	2x+2	2x	2x	2x	2x	2	2	2	2
			1	2x+1		0	2x+2	2	2x	3x+3	x+1	3x+1	x+3	2x+1	3	2x+3	1	x	3x+2	x+2	3x
		x+1	0	3x+1		0	0	2x+2	2x+2	2	2	2x	2x	3x+1	3x+1	x+3	x+3	3x+3	3x+3	x+1	x+1
			1	3x+2		0	2x+2	2x	2	x+3	3x+1	3x+3	x+1	3x+2	x	x+2	3x	1	2x+3	2x+1	3

Figure 11. Field matrix resulting from $Z_4[x]$ mod x^2+1 with the map $1 \mapsto -1$, $x+1 \mapsto i$

	0	2x+2	2	2x	x+1	3x+3	x+3	3x+1	1	2x+3	3	2x+1	x+2	3x	x	3x+2
0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	-1	1	-1	-i	i	-i	i	-1	1	-1	1	i	-i	i	-i
x+1	1	1	-1	-1	-1	-1	1	1	-i	-i	i	i	i	i	-i	-i
x+2	1	-1	-1	1	i	-i	-i	i	i	-i	-i	i	-1	1	1	-1
2	1	1	1	1	-1	-1	-1	-1	1	1	1	1	-1	-1	-1	-1
3	1	-1	1	-1	i	-i	i	-i	-1	1	-1	1	-i	i	-i	i
x+3	1	1	-1	-1	1	1	-1	-1	-i	-i	i	i	-i	-i	i	i
x	1	-1	-1	1	-i	i	i	-i	i	-i	-i	i	1	-1	-1	1
2x+2	1	1	1	1	1	1	1	1	-1	-1	-1	-1	-1	-1	-1	-1
2x+3	1	-1	1	-1	-i	i	-i	i	1	-1	1	-1	-i	i	-i	i
3x+3	1	1	-1	-1	-1	-1	1	1	i	i	-i	-i	-i	-i	i	i
3x	1	-1	-1	1	i	-i	-i	i	-i	i	i	-i	1	-1	-1	1
2x	1	1	1	1	-1	-1	-1	-1	-1	-1	-1	-1	1	1	1	1
2x+1	1	-1	1	-1	i	-i	i	-i	1	-1	1	-1	i	-i	i	-i
3x+1	1	1	-1	-1	1	1	-1	-1	i	i	-i	-i	i	i	-i	-i
3x+2	1	-1	-1	1	-i	i	i	-i	-i	i	i	-i	-1	1	1	-1

matrix, although the assignments (see figure 11) 1 |-> -1, x+1 |-> i allow the field matrix to factor into a nonsingular 16x16 matrix using all the fourth roots of unity.

Another example comes from the ring of 2x2 matrices over Z_2, (see figure 12). This noncommutative ring can have its columns factored by the chain R $\{^{00\ 00\ 00\ 00}_{00,10,01,11}\}$, with the annihilator chain {0} $\{^{00\ 00\ 10\ 10}_{00,10,00,10}\}$. This splits the matrix into sixteen 4x4 subblocks which unfortunately cannot be factored further by a column subring which can be annihilated. However, the assignments $^{01\ 00}_{00,10}$ |-> -1, and $^{10\ 00}_{00,01}$ |-> 1 produce a 16x16 Hadamard matrix.

Finally, we give an example using the orthogonality of the basis for $\otimes_k Z_2$ to get a resulting field matrix with entries not being roots of unity. Observe figure 2 for the ring $\otimes_k Z_2$, previously associated with the Hadamard transform. If we map all the basis elements {1,2,4,8} to zero, then we will produce a recursive matrix in the field

$$P_{n+1} = \begin{bmatrix} P_n & P_n \\ P_n & 0 \end{bmatrix} \qquad P_1 = 1$$

with zero (not a root of unity) occurring in the matrix. This transform was used by Cull in calculating statistics of neural nets.

Figure 12. Factorization of the ring of 2x2 matrices over Z_2

			S				10 00 + S				01 00 + S				11 00 + S			
A	L		00 00	00 10	00 01	00 11	10 00	10 10	10 01	10 11	01 00	01 10	01 01	01 11	11 00	11 10	11 01	11 11
00 00	00 00	00 00	00 00	00 00	00 00	00 00	00 00	00 00	00 00	00 00	00 00	00 00	00 00	00 00	00 00	00 00	00 00	00 00
	00 01	00 01	00 00	00 10	00 01	00 11	00 00	00 10	00 01	00 11	00 00	00 10	00 01	00 11	00 00	00 10	00 01	00 11
	01 00	01 00	00 00	10 00	01 00	11 00	00 00	10 00	01 00	11 00	00 00	10 00	01 00	11 00	00 00	10 00	01 00	11 00
	01 01	01 01	00 00	10 10	01 01	11 11	00 00	10 10	01 01	11 11	00 00	10 10	01 01	11 11	00 00	10 10	01 01	11 11
00 10	00 00	00 10	00 00	00 00	00 00	00 00	00 10	00 10	00 10	00 10	00 01	00 01	00 01	00 01	00 11	00 11	00 11	00 11
	00 01	00 11	00 00	00 10	00 01	00 11	00 10	00 00	00 11	00 01	00 01	00 11	00 00	00 10	00 11	00 01	00 10	00 00
	01 00	01 10	00 00	10 00	01 00	11 00	00 10	10 10	01 10	11 10	00 01	10 01	01 01	11 01	00 11	10 11	01 11	11 11
	01 01	01 11	00 00	10 10	01 01	11 11	00 10	10 00	01 11	11 01	00 01	10 11	01 00	11 10	00 11	10 01	01 10	11 00
10 00	00 00	10 00	00 00	00 00	00 00	00 00	10 00	10 00	10 00	10 00	01 00	01 00	01 00	01 00	11 00	11 00	11 00	11 00
	00 01	10 01	00 00	00 10	00 01	00 11	10 00	10 10	10 01	10 11	01 00	01 10	01 01	01 11	11 00	11 10	11 01	11 11
	01 00	11 00	00 00	10 00	01 00	11 00	10 00	00 00	11 00	01 00	01 00	01 00	00 00	10 00	11 00	01 00	10 00	00 00
	01 01	11 01	00 00	10 10	01 01	11 11	10 00	00 10	10 11	01 11	01 00	11 10	00 01	10 11	11 00	01 10	10 01	00 11
10 10	00 00	10 10	00 00	00 00	00 00	00 00	10 10	10 10	10 10	10 10	01 01	01 01	01 01	01 01	11 11	11 11	11 11	11 11
	00 01	10 11	00 00	00 10	00 01	00 11	10 10	10 00	10 11	10 01	01 01	01 11	01 00	01 10	11 11	11 01	11 10	11 00
	01 00	11 10	00 00	10 00	01 00	11 00	10 10	00 10	11 10	01 10	01 01	11 01	00 01	10 01	11 11	01 11	10 11	00 11
	01 01	11 11	00 00	10 10	01 01	11 11	10 10	00 00	11 11	01 01	01 01	11 11	00 00	10 10	11 11	01 01	10 10	00 00

where the columns are factored by the subring

$$R = \{\begin{smallmatrix}00\\00\end{smallmatrix}, \begin{smallmatrix}00\\10\end{smallmatrix}, \begin{smallmatrix}00\\01\end{smallmatrix}, \begin{smallmatrix}00\\11\end{smallmatrix}\}$$

where the rows are factored by the annihilator subring

$$A = \{\begin{smallmatrix}00\\00\end{smallmatrix}, \begin{smallmatrix}00\\10\end{smallmatrix}, \begin{smallmatrix}10\\00\end{smallmatrix}, \begin{smallmatrix}10\\10\end{smallmatrix}\}$$

Chapter IV

The Use of Infinite Rings to Produce Finite Factorable Field Matrices

If we limit ourselves to the factorization of finite rings, is there a direct correspondence of rings with matrices factored in the form of figure 5b? Suppose we pick for a field matrix the upper left quadrant of the matrix shown in figure 13b, which is produced from the ring multiplication table for Z_9 (shown in figure 13a) mapped by the natural homomorphism from Z_9 to the powers of the principal ninth root of unity. Unfortunately, this matrix has all the distinct ninth roots of unity occurring as entries, which is too many for a six element ring's table to produce. This suggests allowing the deletion of some of the rows and columns of the ring's multiplication table, before mapping the table into a field matrix.

As previously stated, a factorable field matrix can be obtained from a factorable finite ring's multiplication table if the exponential mapping is a homomorphism, or if four conditions including orthogonality of the basis elements are met. Homomorphism implies mapping the ring basis elements to roots of unity, whereas the orthogonality conditions allow the ring basis elements to be mapped to arbitrary elements of the field. Selective deletion of elements and groups of elements from the row and column entries of the table not only will allow ring factorization of matrices of the sort of figure 13b, but

Figure 13a. Factorization of Z_9 with column factoring subring and annihilator subring

$S = A = \langle 3 \rangle = \{0,3,6\}$

A	L		$\langle 3 \rangle$			$1+\langle 3 \rangle$			$2+\langle 3 \rangle$		
			0	3	6	1	4	7	2	5	8
	0	0	0	0	0	0	0	0	0	0	0
0	1	1	0	3	6	1	4	7	2	5	8
	2	2	0	6	3	2	8	5	4	1	7
	0	3	0	0	0	3	3	3	6	6	6
3	1	4	0	3	6	4	7	8	8	2	5
	2	5	0	6	3	5	2	8	1	3	1
	0	6	0	0	0	6	6	6	3	3	3
6	1	7	0	3	6	7	1	4	5	8	2
	2	8	0	6	3	8	5	2	7	4	1

Figure 13b. Natural map of Z_9 factorization to the ninth roots of unity

1	1	1	1	1	1	1	1	1
1	w_3	w_6	w	ww_3	ww_6	w_2	w_2w_3	w_2w_6
1	w_6	w_3	w_2	w_2w_6	w_2w_3	w_4	w_4w_6	w_4w_3
1	1	1	w_3	w_3	w_3	w_6	w_6	w_6
1	w_3	w_6	w_4	w_4w_3	w_4w_6	w_8	w_8w_3	w_8w_6
1	w_6	w_3	w_5	w_5w_6	w_5w_3	w	ww_6	ww_3
1	1	1	w_6	w_6	w_6	w_3	w_3	w_3
1	w_3	w_6	w_7	w_7w_3	w_7w_6	w_5	w_5w_3	w_5w_6
1	w_6	w_3	w_8	w_8w_6	w_8w_3	w_7	w_7w_6	w_7w_3

also will allow the use of characteristic zero rings which make no special requirement on the exponential map or basis of the ring in order to guarantee the factorization of the field matrix, since there is no cancellation problem under addition in the ring.

With a characteristic zero ring we are immediately struck by the problem of an infinite number of elements factoring into possibly an infinite number of infinite size cosets. For the basic column factoring set we use a carefully selected finite subset of a parent factoring subring. In addition, we only use a selected finite number of the possible shrunken cosets of the factorization.

Are there infinite rings from which we can construct a factorable finite table? Consider the ring of nxn matrices over the integers. The chain of parent subrings which factor the 'columns' of the table will be nilpotent matrices of the following form, $R=S_0 \supset S_1 \supset S_2 \supset \ldots \supset S_{n-2}$, where S_i is upper triangular with nonzero entries occurring only in columns two through n-i. The S_i are subrings since they are closed under addition and multiplication, and contain the element zero. Note that S_1 leaves the last column as zeroes, a convenience for annihilation. The annihilator chain $\{0\} \subset A_1 \subset A_2 \subset \ldots \subset A_{n-2}$, have the A_i being lower triangular nilpotent matrices with nonzero entries occurring only in columns i+1 through n-1. Observe that A_i does not annihilate S_j

for i>j, which is what we want if the annihilator rings are to be maximal and distinct.

Is it possible to select a portion of the above rings infinite factored table to arrive at a finite table translating to a useful field matrix? For our parent column factoring subrings we select $R \supset S_1 \supset S_2$, with the elements b=c=g=1.

$$S_1 = \begin{bmatrix} 0 & b & c & 0 \\ 0 & 0 & g & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad S_2 = \begin{bmatrix} 0 & b & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

For the parent annihilator subrings select $\{0\} \subset A_1 \subset A_2$, with the elements j=n=x=1.

$$A_1 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & x & 0 \end{bmatrix} \qquad A_2 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & j & 0 & 0 \\ 0 & n & x & 0 \end{bmatrix}$$

If we represent 4x4 matrices which have a value 1 in a particular entry by a string of characters representing the sixteen positions as:

$$\begin{bmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & x & p \end{bmatrix} \qquad ick = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Using this notation we can depict a selected finite field table for this parent ring structure as in figure 14. This factorization gives to a Hadamard matrix with the mapping x |-> 1, j,p |-> -1. The mapping x |-> 1, j,p |-> 0, gives the example zero/one matrix.

Figure 14. Multiplication table of finite selection of characteristic zero ring.

				S_1				$1+S_1$			
				S_2		$g+S_2$					
A_1	A_2	L		0	b	g	gb	1	1b	1g	1gb
0	0	0	0	0	0	0	0	0	0	0	0
		i	i	0	j	0	j	0	j	0	j
	n	0	n	0	0	x	x	0	0	x	x
		i	xi	0	j	x	xj	0	j	x	xj
x	0	0	x	0	0	0	0	0	p	p	p
		i	xi	0	j	0	j	p	pj	p	pj
	n	0	xn	0	0	x	x	p	p	px	px
		i	xni	0	j	x	xj	p	pj	px	pxj

This factorization gives a Hadamard matrix with mapping
x ¦-> 1, j,p ¦-> -1.
The mapping x ¦-> 0, j,p ¦-> 0, gives the example zero/one matrix.

Chapter V

Comparison of Matrices Producable from the Factorization of Rings and from a Generalized Kronecker Product Technique

The factorization of a ring's multiplication table gives an algebraic view of symmetry giving fast matrix multiplication. There exist generative techniques which build matrices directly from submatrices of the field which cannot be produced by a mapping from a ring's multiplication table.

Fino and Algazi present a technique utilizing a 'generalized' Kronecker product. For a set $\{A^i\}$ $i=0,1,\ldots,m-1$ of m nxn matrices, and a set $\{B^j\}$ $j=0,1,\ldots,n-1$ of n mxm matrices, an mn x mn matrix is produced using the following operations:

1) row and column permutations
2) multiplication of rows or columns by a root of unity (or constant)
3) generalized Kronecker product, using sets $\{A^i\}$ and $\{B^j\}$, define $\{A\} \otimes \{B\}$ to be the square matrix C of order mn x mn such that:

$$C_{i,j} = C_{um+w,u'm+w'} = A^{w}_{u,u'} * B^{u'}_{w,w'} \quad \text{where}$$

$$i = u*m + w, \qquad u,u' = 0,1,\ldots,n-1$$

$$j = u'*m + w', \qquad w,w' = 0,1,\ldots,m-1$$

These generative rules are applied recursively to build a fast matrix. See figure 15 for pictorial representation of the generalized Kronecker product. In the case that

Figure 15. The generallized Kronecker product of two sets of matrices $\{A^i\}$ and $\{B^j\}$ denoted by $\{A\} \otimes \{B\}$ can be represented in block matrix form by:

$$\begin{bmatrix}
D_{00}B_0 & D_{01}B_1 & D_{02}B_2 & \cdots & D_{0,n-1}B_{n-1} \\
D_{10}B_0 & D_{11}B_1 & D_{12}B_2 & \cdots & D_{1,n-1}B_{n-1} \\
D_{20}B_0 & D_{21}B_1 & D_{22}B_2 & \cdots & D_{2,n-1}B_{n-1} \\
D_{30}B_0 & D_{31}B_1 & D_{32}B_2 & \cdots & D_{3,n-1}B_{n-1} \\
\vdots & \vdots & \vdots & & \vdots \\
D_{m-1,0}B_0 & D_{m-1,1}B_1 & D_{m-1,2}B_2 & \cdots & D_{m-1,n-1}B_n
\end{bmatrix}$$

where the diagonal matrices D_{ij} have their entries taken from the A^i matrices as follows:

$$D_{ij} = \begin{bmatrix}
A_{ij}^0 & & & & & & \\
& A_{ij}^1 & & & & & \\
& & A_{ij}^2 & & & & \\
& & & A_{ij}^3 & & & \\
& & & & A_{ij}^4 & & \\
& & & & & \ddots & \\
& & & & & & A_{ij}^{m-1}
\end{bmatrix}$$

all the A^i in the set $\{A^i\}$ are identical, and all the B^j in the set $\{B^j\}$ are identical, this definition produces the normal Kronecker product.

The important differences between the factored field matrices produced by the generalized Kronecker technique and the ring table technique are made evident by examining the comparison in figure 16. The ring technique has a single subblock X occurring throughout the matrix which is modified by a fixed diagonal matrix for each column of subblocks of the factorization premultiplied by a different scalar element for each subblock of the matrix. The first column of subblocks can be viewed as having the identity as the diagonal matrix, premultiplied by the scalar value one. The generalized Kronecker product allows a different basic subblock for each column of subblocks of a given stage, which requires the same number of subblock matrix multiplications as with the ring's field matrix. Also, each subblock of the matrix is premultiplied by an distinct diagonal matrix. This factorization gives fast multiplication with the same operation count, but with more generality than that of the ring approach.

When applied to actual example transforms, the set $\{B^j\}$ usually consists of a fixed matrix B. This formulation, by still allowing arbitrary premultiplying diagonals for subblocks, is still more general than the ring approach. However, the ring approach still gives a

Figure 16. The generallized Kronecker product technique of Fino allows the following recursive form for each stage of a factorization of a field matrix.

$$\begin{bmatrix} D_{11}X_1 & D_{12}X_2 & D_{13}X_3 & \cdots & D_{1n}X_n \\ D_{21}X_1 & D_{22}X_2 & D_{23}X_3 & \cdots & D_{2n}X_n \\ D_{31}X_1 & D_{32}X_2 & D_{33}X_3 & \cdots & D_{3n}X_n \\ D_{41}X_1 & D_{42}X_2 & D_{43}X_3 & \cdots & D_{4n}X_n \\ \vdots & \vdots & \vdots & & \vdots \\ D_{m1}X_1 & D_{m2}X_2 & D_{m3}X_4 & \cdots & D_{mn}X_n \end{bmatrix} \quad \begin{bmatrix} V_1 \\ V_2 \\ V_3 \\ V_4 \\ \vdots \\ V_n \end{bmatrix}$$

Recall the general form for a field matrix produced by a mapping for a ring:

$$\begin{bmatrix} c_{11}D_1X & c_{12}D_2X & c_{13}D_3X & \cdots & c_{1n}D_nX \\ c_{21}D_1X & c_{22}D_2X & c_{23}D_3X & \cdots & c_{2n}D_nX \\ c_{31}D_1X & c_{32}D_2X & c_{33}D_3X & \cdots & c_{3n}D_nX \\ c_{41}D_1X & c_{42}D_2X & c_{43}D_3X & \cdots & c_{4n}D_nX \\ \vdots & \vdots & \vdots & & \vdots \\ c_{m1}D_1X & c_{m2}D_2X & c_{m3}D_3X & \cdots & c_{mn}D_nX \end{bmatrix} \quad \begin{bmatrix} V_1 \\ V_2 \\ V_3 \\ V_4 \\ \vdots \\ V_n \end{bmatrix}$$

handle on the structure of the symmetry of the factored matrix.

One example transform having a description using the general Kronecker product is the Haar transform which has an unfactored form as in figure 17. When rearranged by row and column permutations (figure 17), notice that other than 1) the normallizing factors multiplying the rows of the matrix, and 2) the large portions of the matrix masked out with zeroes, this matrix has the symmetric form of the previously discussed Hadamard matrix. In figure 17, the entries 1,2 and 3 represent the first, second and third powers of the square root of two, the letter e represents the number 1. The form can be described by:

$$H_{n+1} = \begin{bmatrix} H_n & I_n * H_n \\ I_n * H_n & -H_n \end{bmatrix} \qquad I_n = \begin{bmatrix} 1 & & \\ & 0 & \\ & & \ddots \\ & & & 0 \end{bmatrix} \qquad H_1 = 1$$

Since the multiplication $I_n * H_n$ times its portion of the column vector is already computed in both cases (except for a negation), the cost for the lower left and upper right subblocks is one multiply and two additions. Thus the recurrence relation for the cost of the computation becomes $T(n) = 2*T(n/2) + O(1)$, which has an $O(n)$ solution as previously mentioned in chapter 1 and solved in the appendix.

Figure 17. Haar transform matrix of order 16

Unfactored form of matrix

e	e	e	e	e	e	e	e	e	e	e	e	e	e	e	e
-e	-e	-e	-e	-e	-e	-e	-e	e	e	e	e	e	e	e	e
0	0	0	0	0	0	0	0	-1	-1	-1	-1	1	1	1	1
-1	-1	-1	-1	1	1	1	1	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	-2	-2	2	2
0	0	0	0	0	0	0	0	-2	-2	2	2	0	0	0	0
0	0	0	0	-2	-2	2	2	0	0	0	0	0	0	0	0
-2	-2	2	2	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	-3	3
0	0	0	0	0	0	0	0	0	0	0	0	-3	3	0	0
0	0	0	0	0	0	0	0	0	0	-3	3	0	0	0	0
0	0	0	0	0	0	0	0	-3	3	0	0	0	0	0	0
0	0	0	0	0	0	-3	3	0	0	0	0	0	0	0	0
0	0	0	0	-3	3	0	0	0	0	0	0	0	0	0	0
0	0	-3	3	0	0	0	0	0	0	0	0	0	0	0	0
-3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Factored by row and column permutations

e	e	e	e	e	e	e	e	e	e	e	e	e	e	e	e
3	-3	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	2	-2	-2	0	0	0	0	0	0	0	0	0	0	0	0
0	0	3	-3	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	-1	-1	-1	-1	0	0	0	0	0	0	0	0
0	0	0	0	-3	3	0	0	0	0	0	0	0	0	0	0
0	0	0	0	-2	-2	2	2	0	0	0	0	0	0	0	0
0	0	0	0	0	0	3	-3	0	0	0	0	0	0	0	0
e	e	e	e	e	e	e	e	-e	-e	-e	-e	-e	-e	-e	-e
0	0	0	0	0	0	0	0	-3	3	0	0	0	0	0	0
0	0	0	0	0	0	0	0	-2	-2	2	2	0	0	0	0
0	0	0	0	0	0	0	0	0	0	3	-3	0	0	0	0
0	0	0	0	0	0	0	0	-1	-1	-1	-1	1	1	1	1
0	0	0	0	0	0	0	0	0	0	0	0	3	-3	0	0
0	0	0	0	0	0	0	0	0	0	0	0	2	2	-2	-2
0	0	0	0	0	0	0	0	0	0	0	0	0	0	-3	3

Chapter VI

Conclusion

In this paper we have investigated the relationship of a ring factorization with the existence of an associated fast transform matrix.

Given a matrix M of elements from a field F, there exists a 'fast' multiplication of M times a column vector V if there exists a finite ring R satisfying the following requirements:

1) the elements of R can be uniquely represented in terms of a minimal additive generating set $\{b_1,\ldots,b_k\}$ which acts like a basis, i.e. for every r in R there exists a unique linear combination of the b_i such that $r = n_1b_1+\ldots+n_kb_k$.
2) there exists a chain of distinct subrings $R=S_0 \supset S_1 \supset \ldots \supset S_k$ where S_{i+1} is maximal factoring S_i, i.e. no larger $S \supset S_{i+1}$ factors S_i. Note: the weaker assumption that the S_i are just subsets leads to the conclusion that the S_i are either subrings or cosets of subrings. Correspondingly there is a chain of distinct maximal annihilator subrings $\{0\} \subset A_1 \subset A_2 \subset \ldots \subset A_k$, for which the product $A_i*S_i=\{0\}$ and the product $A_j*S_i=\{0\}$ for $j>i$.
3) R and F are related by an exponential map f:R->F, such that the range of f is the set {elements of M}, defined on the generators of R by $f(n*b_i)=w_i^n$.
   a) if f is a homomorphism then we have

$f(n_1*b_1+\ldots+n_k*b_k) = w_1^{n_1}*\ldots*w_k^{n_1}$

which guarantees proper factorization in the field matrix. Notice the w's have to be roots of unity.

b) if 1) the 'basis' elements are multiplicatively orthogonal, 2) if the basis elements used to represent the column coset leaders for each stage do not occur in any of the elements of their respective column factoring rings, and 3) the same holds for the annihilator elements and their corresponding factoring leader subsets, then we also are guaranteed factorization in the matrix M without requiring a homomorphism. This eliminates the need for the w's to be roots of unity.

Possibilities other than strictly a) or b) exist to guarantee the proper factorization of the field matrix M. Take the direct product of a ring which is factorable from being orthogonal and another which has a homomorphism, giving us a ring (with operations defined in componentwise fashion) which satisfies neither of the two mentioned sufficient conditions, but which maps to a factorable matrix in the field. This map is defined in componentwise fashion using the appropriate maps for each constituent ring.

4) one necessary requirement for nonsingularity is that the number of row splits not exceed the number of column splits for any stage.

This result can be generallized to infinite rings R by

carefully selecting in bottom up fashion only a finite number of elements from the ring's factored row and column entries.

We might hope for an exact one-to-one correspondence between transform matrices and particular rings, in order to use rings as a classifying tool for fast transform matrices. Instead we find a single ring can be ambiguously interpreted as various distinct matrices (i.e. Chapter III, Figure 8, page 29), or completely distinct rings can map to the same transform matrix, (i.e. rings found in figures 2, 9 and 12 can all map to the Hadamard transform matrix).

If only a single maximal chain for factorization of the ring existed, then a single ring could only correspond to one factorable form of a field matrix. Variability in ring factorization resides in being able to choose different maximal chains to factor the ring. A ring which can be interpreted as being the direct product of several rings has maximal chains by factoring using any permutation of the ring components. Thus, in some sense the ring factorization is commutative, however the matrices obtained from these different orderings are structurally distinct.

An alternative method exists for generating transform matrices from elementary matrices utilizing a generalized Kronecker product. This method allows the generation of a more general class of matrices than the ring factorization

technique, (Chapter V for discussion, Figure 16 for comparison).

Ring factorization provides a useful tool for viewing the structure underlying typical fast transform matrices, but is limited in the allowable structure of the resulting transform matrix and is veiled in the ambiguity of multiple maximal chain factorizations of the ring.

BIBLIOGRAPHY

Cooley, J. W. and Tukey, J. W. 1965. An Algorithm for the Machine Calculation of Complex Fourier Series. Math. Comput. 19, 297-301.

Cull, P. 1977. A Matrix Algebra for Neural Nets. Applied General Systems Research, G.J. Klir ed. Plenum Press: New York, 563-573.

Fino, B. J. and Algazi, V. R. 1977. A Unified Treatment of Discrete Fast Unitary Transforms. SIAM J. Comput. 6, 700-717.

Hungerford T. W. 1974. Algerbra. Holt, Rinehart, and Winston: San Franciso.

McCoy N. H. 1964. The Theory of Rings. MacMillan: New York.

Shore J. E. 1973. On the Application of Haar Functions. IEEE Trans. Comput., 209-216.

APPENDICES

Appendix I

Recurrence Relations

If we examine figure 5b for the general structure of a field matrix arising from a ring's factored multiplication table, we can determine the recurrence relation for the operation count for multiplying a transform matrix times a column vector. For one stage we have to multiply the basic subblock X with n different V_j subvectors, producing n subproblems of size (M/m)x(N/n), where M is the number of rows and m the number of row splits, N is the number of columns and n is the number column splits. After computing these n subproblems, the resulting product subvectors XV_j need to be multiplied by the $c_{ij}D_j$ for i=0,1,...,m-1. Notice that $c_{i1}D_1$ is the identity for the first column of subblocks so we have only (n-1)*m products of a diagonal times a vector to compute. Each of these products requires N/n multiplications for a total of (n-1)*m*N/n multiplications. If we assume that the rows split into m segments and the columns into n segments at every stage, then we arive at a recurrence relation for the operation count T(M,N) for the multiplication of a size MxN matrix multiplying a vector of length N. The recurrence is T(M,N) = n*T(M/m,N/n) + N*m*(n-1)/n. Notice that if N=M and m=n, this recurrence simplifies to T(N) = n*T(N/n) + N*(n-1) which has been referred to in the text.

We can solve the two variable recurrence as follows:

Let $M = m^j$ (be the number of rows), and $N = n^k$ (be the number of columns), then

$$T(j,k) = n*T(j-1,k-1) + n^{k-1}*(n-1)*m$$
$$= n*[n*T(j-2,k-2) + n^{k-2}*(n-1)*m] + n^{k-1}*(n-1)*m$$
$$= n^2*T(j-2,k-2) + 2n^{k-1}*(n-1)*m$$
$$= n^2[n*T(j-3,k-3) + n^{k-3}*(n-1)*m] + 2n^{k-1}*(n-1)*m$$
$$= n^3T(j-3,k-3) + 3n^{k-1}*(n-1)*m$$

For $j <= k$ this leads to

$$T(j,k) = n^j*T(0,k-j) + j*n^{k-1}(n-1)*m$$
$$= n^{\log_m M}*T(0,k-j) + j*n^{k-1}*(n-1)*m$$
$$= n^{\log_m M}*T(0,k-j) + (n-1)/n*\log_m M*m*N$$
$$= M^{\log_m n}*T(0,k-j) + (n-1)/n*m*\log_m M*N$$

Assuming M=N to begin with:

we have that since $j<=k$, then $m>=n$

so that $\log_m n <= 1$ implying $M^{\log_m n} <= N$

$$T(j,k) = O(N\log M)$$

In particular, if M=N and m=n, then

$M^{\log_m n} = N$ which implies

$T(j,k) = T(j) = O(N\log N)$ for an equal row and column split recursive breakdown.

If $j>=k$ then

$$T(j,k) = n^k*T(j-k,0) + (n-1)/n*j*m*n^k$$
$$= N*T(j-k,0) + (n-1)/n*m*\log_m M*N$$
$$= O(N\log M)$$

Again considering the case where N=M and n=m, we have an $O(N\log N)$ solution.

If we have the recurrence relation for the fast Haar

transform, $T(n) = 2*T(n/2) + O(1)$, then

$T(k) = 2*T(k-1) + c$

$= 2*[2*T(k-2) + c] + c$

$= 2^2*T(k-2) + 2c + c$

$= 2^2*[2*T(k-3) + c] + 2c + c$

$= 2^3*T(k-3) + 2^2c + 2c + c$

.

$= 2^k*T(0) + (2^k-1)c$

$= O(N)$

as previously mentioned.

Appendix II

Definitions

Annihilator: For a ring, an element annihilates a subring or subset if when the product of the given element with any element of the subset or subring produces the zero element.

Basis: For a vector space, a basis is a set of elements such that every element of the vector space has a unique representation as a linear combination of the basis elements.

Coset: Given a subgroup S of a group G, we can partition G by taking as the first equivalence class the elements of S, then for the second the sum of the elements of S with an element g_1 not in S, i.e. g_1+S, for the next class the sum of S with an element g_2 not in S or g_1+S, and so on until S is covered. The fact that S is a subgroup guarantees that the preceding sets are pairwise disjoint and thus are the equivalence classes of a partition. The sets g_i+S are called cosets of S. The elements g_i are called coset leaders.

Coset leader: Given a coset g_i+S of the group G, the element g_i is called a coset leader and is not unique. Any element in the coset g_i+S when added to S will give the same set as g_i+S, which implies that there are $|S|$ possible coset leaders for each coset. A set of representative coset leaders is a collection

of elements, one from each distinct coset of S in G.

Direct Product (S O R): Given two rings S and R, we produce a new ring using ordered pairs of elements of S and R where multiplication and addition are the componentwise operations of S and R, i.e. $(s_1,r_1)*(s_2,r_2) = (s_1*s_2,r_1*r_2)$. This can be generalized to any number of components, e.g. O_kZ_n.

Group: A set G with a binary operation +:GxG->G such that 1) the operation is associative, 2) an identity element exists, and 3) inverses exist for all elements. If the binary operation is commutative, then the group is called Abelian. If the binary operation only satisfies associativity, then the structure is called a semigroup.

Homomorphism: A mapping which relates two algebraic structures by requiring that the image of the product of two elements in the first structure is equal to the product in the second structure of the images of the two elements in the first structure, i.e. $f(a*_1b) = f(a)*_2f(b)$ where $*_1$ is the binary operation of the first structure and $*_2$ is the binary operation of the second structure.

Ideal: For a commutative ring R, an ideal I is a subring of R such that for any r in R, r*I I. A principal ideal is one which is generated by a single element, i.e. for some w in I, R*w = I.

Kronecker Product: Given two matrices A and B, the

Kronecker product A ⊗ B is the matrix which has each element a_{ij} of A replaced by the matrix a_{ij}*B.

Ring: A ring is an algebraic stucture with two binary operations, an addition which forms an Abelian group and a multiplication which forms a semigroup. Also, the multiplication distributes over the addition.

Subring: A subset W of a ring R such that W is closed under addition and multiplication, and contains additive inverses for all elements.

Subgroup: A subset S of a group G which is closed under the binary operation and contains inverses for all the elements of S.