Current address & affiliation
Professor Emeritus,
CSE Department
UC San Diego
baden@ucsd.edu

DFT → FFT transformation in FP

Scott B. Baden

University of California, Berkeley

May 3, 1983

1. Introduction

Backus' functional language FP[1] has an underlying algebra that can be used to optimize its programs through source-to-source transformations. Following the well-known textbook derivation of the Fast Fourier Transform (FFT) from the Discrete Fourier Transform (DFT)[2], a DFT program written in FP will be transformed into an equivalent FFT one using only algebraic-style source-to-source transformations.

2. Standard Derivation

Equation (2.1) defines the DFT. R is the index of a the desired frequency component, B and A are a complex-valued Fourier transform pair, $W_N = \exp^{-j2\pi/N}$, $j = \sqrt{-1}$, and N is an integral power of two.

$$A_r = \sum_{k=0}^{N-1} B_k W_N^{rk} \tag{2.1}$$

Replace N by $2M$:

$$A_r = \sum_{k=0}^{2M-1} B_k W_{2M}^{rk} \tag{2.2}$$

Regrouping and expanding:

$$A_r = \sum_{k=0}^{M-1} B_{2k} W_{2M}^{2rk} + \sum_{k=0}^{M-1} B_{2k+1} W_{2M}^{r(2k+1)} \tag{2.3}$$

Since

$$W_{2M}^{2rk} = W_M^{rk} \tag{2.4}$$

and

$$W_{2M}^{r(2k}+1) = W_M^{rk} \cdot W_{2M}^{r} \tag{2.5}$$

Rewriting:

$$A_r = \sum_{k=0}^{M-1} B_{2k} W_M^{rk} + \sum_{k=0}^{M-1} B_{2k+1} W_M^{rk} W_{2M}^{r} \tag{2.6}$$

Next we define:

$$F_{even} \equiv \sum_{k=0}^{M-1} B_{2k} W_M^{rk} \tag{2.7}$$

$$F_{odd} \equiv \sum_{k=0}^{M-1} B_{2k+1} W_M^{rk} \tag{2.8}$$

F_{even} and F_{odd} are, respectively, the $M\text{-}point$ transforms of the even and odd components of the input.

Using (2.7) and (2.8) re-write (2.6) as:

$$F_{even} + W_{2M}^{r} F_{odd} \quad \blacksquare \tag{2.9}$$

3. FP Definition

The discrete Fourier Transform is the dot (inner) product of the input vector, B and and appropriate vector of "twiddle factors" W.

$$\mathbf{dft} \triangleq ip \circ [B\ ,\ \alpha W \circ distl \circ [N\ ,\ svMpy \circ [r\ ,\ iota \circ N]]] \tag{3.1}$$

Inner product function:

$$ip \triangleq (tree\ +) \circ \alpha\times \circ trans \tag{3.2}$$

Scalar-vector multiplication.

$$svMpy \triangleq \alpha\times \circ distl \tag{3.3}$$

Miscellaneous selector functions. N represents the length of the input vector.

$$B \triangleq 1, \qquad r \triangleq 2, \qquad N \triangleq length \circ B \tag{3.4}$$

W calculates the "twiddle" factors:

$$W \triangleq \div \circ [exp \circ \times \circ [negTwoPiJ\ , p\ ]\ ,\ n\ ] \tag{3.5}$$

$$n \triangleq 1, \qquad p \triangleq 2 \tag{3.6}$$

$$negTwoPiJ \triangleq /\times \circ [\overline{-2}, \overline{\pi}, \overline{j}], \quad \textbf{where } j = \sqrt{-1} \tag{3.7}$$

4. FP Derivation

An auxiliary function H is defined to simplify the derivation:

$$H \triangleq \alpha W \circ distl \circ [N\ , svMpy \circ [r\ , iota \circ N]] \tag{4.1}$$

Using this auxiliary function we can redefine $\mathbf{dft}$:

$$\mathbf{dft} \triangleq ip \circ [B\ , H] \tag{4.2}$$

As in § 2, we define $N = 2\times M$:

$$N \equiv \times \circ [\overline{2}, M]. \tag{4.3}$$

Substituting (4.3) into (4.1):

$$H' \triangleq \alpha W \circ distl \circ [\times \circ [\overline{2}, M], svMpy \circ [r\ , iota \circ \times \circ [\overline{2}, M]]] \tag{4.4}$$

Dft is redefined using H':

$$dft \triangleq ip \circ [B\, ,H'] \tag{4.5}$$

Two extraction functions *evens* and *odds* are defined. They select, respectively, the even and odd numbered elements of a sequence:

$$evens : \langle x_0, x_1, \ldots, x_{n-1} \rangle \equiv \langle x_0, x_2, \ldots, x_{n-2} \rangle \tag{4.6}$$

$$odds : \langle x_0, x_1, \ldots, x_{n-1} \rangle \equiv \langle x_1, x_3, \ldots, x_{n-1} \rangle \tag{4.7}$$

The FP definitions for *evens* and *odds* are:

$$evens \triangleq 1 \circ trans \circ pair \tag{4.8}$$

$$odds \triangleq 2 \circ trans \circ pair \tag{4.9}$$

An *object-level* derivation[3] verifies the definition of *evens*:

$$evens : \langle x_0, x_1, \ldots, x_{n-1} \rangle \equiv 1 \circ trans \circ pair : \langle x_0, x_1, \ldots, x_{n-1} \rangle \tag{4.10}$$

$$\equiv 1 \circ trans : \langle \langle x_0, x_1 \rangle, \langle x_2, x_3 \rangle, \ldots, \langle x_{n-2}, x_{n-1} \rangle \rangle \tag{4.11}$$

$$\equiv 1 : \langle \langle x_0, x_2, \ldots, x_{n-2} \rangle, \langle x_1, x_3, \ldots, x_{n-1} \rangle \rangle \tag{4.12}$$

$$\equiv \langle x_0, x_2, \ldots, x_{n-2} \rangle \quad \blacksquare \tag{4.13}$$

Verification of *odds* is left to the reader.

Now for a series of Lemmas.

Lemma 1a: The even elements of $iota \circ N$,

$$evens \circ iota \circ N \tag{4.14}$$

may be expressed in an alternative form:

$$\alpha\, multBy2 \circ iota \circ M, \tag{4.15}$$

where

$$multyBy2 \triangleq \times \circ [\bar{2}, id]. \tag{4.16}$$

Proof: In the appendix. ■

Lemma 1b: $odds \circ iota \circ N \equiv \alpha add1 \circ \alpha multBy2 \circ iota \circ M$

where

$$add1 \triangleq + \circ [\bar{1}, id]. \tag{4.17}$$

Proof: Left as a reader exercise ■

Lemma 2: $(tree\, +) \equiv + \circ [(tree\, +) \circ evens, (tree\, +) \circ odds]$.

I.e an alternative way of adding up all the elements of a sequence is to add up all the even-numbered elements and all the odd-numbered elements separately and then add the two sums.

Proof: An informal object-level derivation in the Appendix ■

Now onto Theorem 1:

Theorem 1: $ip \equiv + \circ [ip \circ \alpha evens, ip \circ \alpha odds]$.

Proof: In the Appendix ∎

What Theorem 1 tells us is that the inner product can be calculated by forming the inner products of the even components and the odd components separately and then adding the results.

Using Theorem 1, (3.5) can be expressed in an equivalent form:

$$dft \triangleq ip \circ [B, H'] \equiv + \circ [ip \circ \alpha evens, ip \circ \alpha odds] \circ [B, H'] \qquad (4.18)$$

$$\equiv + \circ [ip \circ [evens \circ B, evens \circ H'], ip \circ [odds \circ B, odds \circ H']] \qquad (4.19)$$

Next, the expressions $evens \circ H'$ and $odds \circ H'$ must be transformed.

Theorem 2a: $evens \circ H' \equiv \alpha W \circ distl \circ [M, svMpy \circ [r, iota \circ M]]$.

Proof: In the Appendix ∎

Theorem 2b:

$odds \circ H' \equiv svMpy \circ [W \circ [N, r], \alpha W \circ distl \circ [M, svMpy \circ [r, iota \circ M]]$.

Proof: In the Appendix ∎

And now the final transformations. For convenience we define

$$dft \triangleq + \circ [F_1, F_2], \text{ where} \qquad (4.20)$$

$$F_1 \triangleq ip \circ [evens \circ B, evens \circ H'] \qquad (4.21)$$

and

$$F_2 \triangleq ip \circ [odds \circ B, odds \circ H'] \qquad (4.22)$$

First, applying Theorem 2a to (4.21):

$$F_1 \equiv ip \circ [evens \circ B, \alpha W \circ distl \circ [M, svMpy \circ [r, iota \circ M]]]. \qquad (4.23)$$

$$\equiv dft \circ [evens \circ B, r], \qquad (4.24)$$

e.g. the dft of the even-numbered components, since

$$length \circ evens \circ B = M. \qquad (4.25)$$

(this is true because N is an integral power of two).

Applying Theorem 2b to (4.22):

$$F_2 \equiv ip \circ [odds \circ B, Q] \qquad (4.26)$$

where

$$Q \triangleq svMpy \circ [W \circ [N, R], \alpha W \circ distl \circ [M, svMpy \circ [r, iota \circ M]]] \qquad (4.27)$$

(4.27) may be simplified using Lemma 5.

Lemma 5: The inner product of two vectors, $\vec{x}$ and $k\vec{y}$ where k is an arbitrary constant, is the same as the product of k and the inner product of the two vectors. In ordinary mathematical terms:

$$\vec{x} \cdot k\vec{y} = k \times (\vec{x} \cdot \vec{y}) \tag{4.28}$$

In FP:

$$ip \circ [\vec{x}\, , svMpy \circ [k\, , \vec{y}]] \equiv \times \circ [k\, , ip \circ [\vec{x} , \vec{y}]] \tag{4.29}$$

Proof: In the appendix $\blacksquare$

Applying Lemma 5 to (4.26):

$$F_2 \equiv \times \circ [W \circ [N, r], ip \circ [odds \circ B\, , \alpha W \circ distl \circ [M\, , svMpy \circ [r, iota \circ M]]]] \tag{4.30}$$

(4.30) is equivalent to multiplying the dft of the odd components of the input by $W \circ [N, r]$:

$$\equiv \times \circ [W \circ [N, r], dft \circ [odds \circ B, r]] \tag{4.31}$$

since $length \circ odds \circ B \equiv M$.

Substituting (4.24) and (4.31) back into (4.20):

$$dft \triangleq + \circ [dft \circ [evens \circ B, r], \times \circ [W \circ [N, r], dft \circ [odds \circ B, r]]] \quad \blacksquare \tag{4.32}$$

5. References

1. John Backus, "Can Programming be Liberated from the von Neumann Style? A Functional Style and its Algebra of Programs," *CACM* Vol. **21**(8), pp. 613-641, 1977 ACM Turing Award Lecture (August 1978).
2. R. C. Gonzalez and P. Wintz, *Digital Image Procesing*, Addison-Wesley, Reading, MA (1981).
3. John Backus, "Functions as Mathematical Objects," *Proc. Conf. Functional Languages and Computer Architecture*, ACM (1981).

6. Appendix of Proofs

Most of the Theorems and Lemmas are by no means general – they work over only a restricted domain of inputs under the assumption that all the computations converge. This was done in the interest of keeping the proofs short. Such an approach is realistic since the task at hand is to transform a *correct* program that operates over a restricted domain of inputs (*e.g.* for inputs consisting of vectors whose lengths are integral powers of two). The proofs consist of derivations involving equivalences of *function-level* expressions and, from time to time, *value-level* ones. Although it would be more desirable to use only function-level derivations, FP's lack of bound variables makes the task extremely difficult if not impossible.

In the derivations equivalences will be made between two function-level expressions, two value-level expressions, or a function-level and a value-level expression. The first two types of equivalences will be called "ordinary" equivalences, while the latter one will be called a "mixed" equivalence. Mixed equivalences involve an implicit application of the function-level expression to a "typical" value chosen from an appropriately restricted domain *e.g.* the one over which the theorem or lemma is defined. Such an equivalence represents a value-level equivalence between the result of the "typical" application and the value-level expression provided. Put differently, mixed equivalences stand for value-level equivalences between a given value expression and the value that would result from applying the given function expression to a representative element of the domain over which the equivalence is defined. Using Backus' terminology[3], the function-level expression could be viewed as the "lift" of the value-level expression. Here the equivalence has been made at the function-level. To emphasize the basic difference between mixed equivalences and ordinary ones, the symbol $\cong$ is used instead of the symbol $\equiv$. In light of the above the correspondence

$$\mathit{iota} \circ N \cong \mathit{iota} : n \tag{6.1}$$

is valid so long as $\mathit{iota} \circ N$ is applied to a sequence of length n (remember that $N \triangleq \mathit{length} \circ 1$). This particular substitution of n for N (and N for n) is used throughout the derivations as is the substitution of m for M and M for m. The substitution of the value-level symbols n and m for N and M can be made under the restricted domain of sequences of length n; *e.g.* $n = N : \langle x_0, x_1, \ldots, x_{n-1} \rangle$.

Lemma 1a: $\mathit{evens} \circ \mathit{iota} \circ N \equiv \alpha\mathit{multBy}2 \circ \mathit{iota} \circ M$.

Proof:

$$\mathit{evens} \circ \mathit{iota} \circ N \cong 1 \circ \mathit{trans} \circ \mathit{pair} \circ \mathit{iota} : n \tag{6.2}$$

$$\equiv 1 \circ \mathit{trans} : \langle \langle 0,1 \rangle, \langle 2,3 \rangle, \ldots, \langle n-2, n-1 \rangle \rangle \tag{6.3}$$

$$\equiv 1 : \langle \langle 0,2,4, \ldots, n-2 \rangle, \langle 1,3,5, \ldots, n-1 \rangle \rangle \tag{6.4}$$

$$\equiv \langle 0,2,4, \ldots, n-2 \rangle \tag{6.5}$$

But $n = 2m$:

$$\equiv \langle 0,2,4, \ldots, 2m-2 \rangle \tag{6.6}$$

$$\equiv \langle 2\times 0, 2\times 1, 2\times 2, \cdots, 2\times(m-1) \rangle \tag{6.7}$$

$$\equiv \alpha\mathit{multBy}2 : \langle 0,1, \ldots, m-1 \rangle \tag{6.8}$$

$$\cong \alpha\mathit{multBy}2 \circ \mathit{iota} \circ M \quad \blacksquare \tag{6.9}$$

Lemma 2: $(\mathit{tree}\,+) \equiv + \circ [(\mathit{tree}\,+) \circ \mathit{evens}, (\mathit{tree}\,+) \circ \mathit{odds}]$.

Proof:

$$+ \circ [(\mathit{tree}\,+) \circ \mathit{evens}, (\mathit{tree}\,+) \circ \mathit{odds}] : \langle x_0, x_1, \ldots, x_{n-1} \rangle \tag{6.10}$$

$$\equiv + \circ \alpha(\mathit{tree}\,+) \circ [\mathit{evens}, \mathit{odds}] : \langle x_0, x_1, \ldots, x_{n-1} \rangle \tag{6.11}$$

$$\equiv + \circ \alpha(\mathit{tree}\,+) : \langle \langle x_0, x_2, \ldots, x_{n-2} \rangle, \langle x_1, x_3, \ldots, x_{n-1} \rangle \rangle \tag{6.12}$$

$$\equiv + : \langle x_0 + x_2 + \cdots + x_{n-2}, x_1 + x_3 + \cdots + x_{n-1} \rangle \tag{6.13}$$

$$\equiv x_0 + x_2 + \cdots + x_{n-2} + x_1 + x_3 + \cdots + x_{n-1} \tag{6.14}$$

$$\equiv x_0 + x_1 + \cdots + x_{n-2} + \cdots + x_{n-1} \tag{6.15}$$

$$\equiv (\mathit{tree}\,+) : \langle x_0, x_1, \ldots, x_{n-1} \rangle \tag{6.16}$$

$$\cong (tree +) \quad \blacksquare \tag{6.17}$$

The last step is legal since it is assumed that addition is both commutative and associative.

Lemma 3a: *evens* ∘ *trans* ≡ *trans* ∘ α*evens*

Proof:

$$evens \circ trans : \langle\langle x_0, x_1, \ldots, x_{n-1}\rangle, \langle y_0, y_1, \ldots, y_{n-1}\rangle\rangle \tag{6.18}$$

$$\equiv evens : \langle\langle x_0, y_0\rangle, \ldots, \langle x_{n-1}, y_{n-1}\rangle\rangle \tag{6.19}$$

$$\equiv \langle\langle x_0, y_0\rangle, \langle x_2, y_2\rangle, \ldots, \langle x_{n-2}, y_{n-2}\rangle\rangle \tag{6.20}$$

$$\equiv trans : \langle\langle x_0, x_2, \ldots, x_{n-2}\rangle, \langle y_0, y_2, \ldots, y_{n-2}\rangle\rangle \tag{6.21}$$

$$\equiv trans \circ \alpha evens : \langle\langle x_0, x_1, \ldots, x_{n-1}\rangle, \langle y_0, y_1, \ldots, y_{n-1}\rangle\rangle \tag{6.22}$$

$$\cong trans \circ \alpha evens \quad \blacksquare \tag{6.23}$$

Lemma 3b: *odds* ∘ *trans* ≡ *trans* ∘ α*odds*

Proof: Left to the reader ■

Lemma 4a: *evens* ∘ *distl* ≡ *distl* ∘ [1,*evens* ∘ 2]

Proof:

$$evens \circ distl : \langle x, \langle y_0, y_1, \ldots, y_{n-1}\rangle\rangle \equiv \tag{6.24}$$

$$\equiv evens : \langle\langle x, y_0\rangle, \langle x, y_1\rangle, \cdots, \langle x, y_{n-1}\rangle\rangle \tag{6.25}$$

$$\equiv \langle\langle x, y_0\rangle, \langle x, y_2\rangle, \cdots, \langle x, y_{n-2}\rangle\rangle \tag{6.26}$$

$$\equiv distl : \langle x, \langle y_0, y_2, \ldots, y_{n-2}\rangle\rangle \tag{6.27}$$

$$\equiv distl : \langle x, evens : \langle y_0, y_1, \ldots, y_{n-1}\rangle\rangle \tag{6.28}$$

$$\equiv distl \circ [1, evens \circ 2] : \langle x, \langle y_0, y_1, \ldots, y_{n-1}\rangle\rangle \tag{6.29}$$

$$\cong distl \circ [1, evens \circ 2] \quad \blacksquare \tag{6.30}$$

Lemma 4b: *odds* ∘ *distl* ≡ *distl* ∘ [1,*odds* ∘ 2]

Proof: *Left to the reader* ■

Lemma 5: $ip \circ [\vec{x}, svMpy \circ [k, \vec{y}]] \equiv \times \circ [k, ip \circ [\vec{x}, \vec{y}]]$

Proof:

$$ip : \langle\langle x_0, x_1, \ldots, x_{n-1}\rangle, svMpy : \langle k, \langle y_0, y_1, \ldots, y_{n-1}\rangle\rangle\rangle \quad (6.31)$$

$$\equiv ip : \langle\langle x_0, x_1, \ldots, x_{n-1}\rangle, \langle k \cdot y_0, k \cdot y_1, \ldots, k \cdot y_{n-1}\rangle\rangle \quad (6.32)$$

$$\equiv k \cdot x_0 \cdot y_0 + k \cdot x_1 \cdot y_1 + \cdots + k \cdot x_{n-1} \cdot y_{n-1} \quad (6.33)$$

$$\equiv k \times (x_0 \cdot y_0 + x_1 \cdot y_1 + \cdots + x_{n-1} \cdot y_{n-1}) \quad (6.34)$$

$$\equiv \times : \langle k, (tree +) : \langle x_0 \cdot y_0, x_1 \cdot y_1, \cdots, x_{n-1} \cdot y_{n-1}\rangle\rangle \quad (6.35)$$

$$\equiv \times : \langle k, (tree +) : \alpha\times \circ trans : \langle\langle x_0, x_1, \ldots, x_{n-1}\rangle, \langle y_0, y_1, \ldots, y_{n-1}\rangle\rangle\rangle \quad (6.36)$$

$$\cong \times \circ [k, (tree +) \circ \alpha\times \circ trans \circ [\vec{x}, \vec{y}]] \quad (6.37)$$

$$\equiv \times \circ [k, ip \circ [\vec{x}, \vec{y}]] \quad \blacksquare \quad (6.38)$$

Theorem 1: $ip \equiv + \circ [ip \circ \alpha evens, ip \circ \alpha odds]$.

Proof:

$$ip \equiv (tree +) \circ \alpha\times \circ trans \quad (6.39)$$

Using Lemma 2 expand (tree +) into the tree sums of the odd and even elements:

$$\equiv + \circ [(tree +) \circ evens, (tree +) \circ odds] \circ \alpha\times \circ trans \quad (6.40)$$

$$\equiv + \circ \alpha(tree +) \circ [evens, odds] \circ \alpha\times \circ trans \quad (6.41)$$

$$\equiv + \circ \alpha(tree +) \circ [evens \circ \alpha\times, odds \circ \alpha\times] \circ trans \quad (6.42)$$

Now

$$evens \circ \alpha\times \equiv \alpha\times \circ evens \quad (6.43)$$

and

$$odds \circ \alpha\times \equiv \alpha\times \circ odds \quad (6.44)$$

so long as all the computations converge (proofs left to the reader). We now have:

$$ip \equiv + \circ \alpha(tree +) \circ [\alpha\times \circ evens, \alpha\times \circ odds] \circ trans \quad (6.45)$$

$$\equiv + \circ \alpha(tree +) \circ [\alpha\times \circ evens \circ trans, \alpha\times \circ odds \circ trans] \quad (6.46)$$

By Lemmas 3a and 3b

$$evens \circ trans \equiv trans \circ \alpha evens \quad (6.47)$$

and

$$odds \circ trans \equiv trans \circ \alpha odds. \quad (6.48)$$

Application of these Lemmas to (6.46) yields:

$$ip \equiv + \circ \alpha(tree +) \circ [\alpha\times \circ trans \circ \alpha evens, \alpha\times \circ trans \circ \alpha odds] \quad (6.49)$$

$$\equiv + \circ [(tree\ +) \circ \alpha \times \circ trans \circ \alpha evens, (tree\ +) \circ \alpha \times \circ trans \circ \alpha odds] \qquad (6.50)$$

$$\equiv + \circ [ip \circ \alpha evens, ip \circ \alpha odds] \quad \blacksquare \qquad (6.51)$$

Theorem 2a: $evens \circ H' \equiv \alpha W \circ distl \circ [M, svMpy \circ [r, iota \circ M]]$.

Proof:

$$evens \circ H' \equiv evens \circ \alpha W \circ distl \circ [\times \circ [\bar{2}, M], svMpy \circ [r, iota \circ \times \circ [\bar{2}, M]]] \qquad (6.52)$$

$$\equiv \alpha W \circ evens \circ distl \circ [\times \circ [\bar{2}, M], svMpy \circ [r, iota \circ \times \circ [\bar{2}, M]]] \qquad (6.53)$$

But by Lemma 4a,

$$evens \circ distl \equiv distl \circ [1, evens \circ 2]. \qquad (6.54)$$

So $evens \circ H'$

$$\equiv \alpha W \circ distl \circ [1, evens \circ 2] \circ [\times \circ [\bar{2}, M], svMpy \circ [r, iota \circ \times \circ [\bar{2}, M]]] \qquad (6.55)$$

$$\equiv \alpha W \circ distl \circ [\times \circ [\bar{2}, M], evens \circ svMpy \circ [r, iota \circ \times \circ [\bar{2}, M]]] \qquad (6.56)$$

$$\equiv \alpha W \circ distl \circ [\times \circ [\bar{2}, M], evens \circ \alpha \times \circ distl \circ [r, iota \circ \times \circ [\bar{2}, M]]] \qquad (6.57)$$

$$\equiv \alpha W \circ distl \circ [\times \circ [\bar{2}, M], \alpha \times \circ evens \circ distl \circ [r, iota \circ \times \circ [\bar{2}, M]]] \qquad (6.58)$$

Applying Lemma 4a again, and, using the definition of $svMpy$:

$$\equiv \alpha W \circ distl \circ [\times \circ [\bar{2}, M], svMpy \circ [r, evens \circ iota \circ \times \circ [\bar{2}, M]]] \qquad (6.59)$$

$$\equiv \alpha W \circ distl \circ [\times \circ [\bar{2}, M], svMpy \circ [r, svMpy \circ [\bar{2}, iota \circ M]]] \qquad (6.60)$$

But

$$svMpy \circ [r, svMpy \circ [\bar{2}, iota \circ M]] \equiv svMpy \circ [\times \circ [\bar{2}, r], iota \circ M] \qquad (6.61)$$

(the proof is left to the reader). So (6.60) reduces to:

$$\alpha W \circ distl \circ [\times \circ [\bar{2}, M], svMpy \circ [\times \circ [\bar{2}, r], iota \circ M]] \qquad (6.62)$$

$$\cong \alpha W \circ distl : \langle 2m, \langle 2r \cdot 0, 2r \cdot 1, \cdots, 2r \cdot (m-1) \rangle \rangle \qquad (6.63)$$

$$\equiv \alpha W : \langle \langle 2m, 2r \cdot 0 \rangle, \langle 2m, 2r \cdot 1 \rangle, \cdots, \langle 2m, 2r \cdot (m-1) \rangle \rangle \qquad (6.64)$$

$$\equiv \langle W : \langle 2m, 2r \cdot 0 \rangle, W : \langle 2m, 2r \cdot 1 \rangle, \cdots, W : \langle 2m, 2r \cdot (m-1) \rangle \rangle \qquad (6.65)$$

But

$$W^{2r}_{2M} \equiv W^{r}_{M} \qquad (6.66)$$

i.e.

$$W : \langle 2m, 2r \rangle \equiv W : \langle m, r \rangle \qquad (6.67)$$

so (6.65) reduces to:

$$\equiv \langle W : \langle m, r \cdot 0 \rangle, W : \langle m, r \cdot 1 \rangle, \cdots, W : \langle m, r \cdot (m-1) \rangle \rangle \qquad (6.68)$$

$$\equiv \alpha W \circ distl : \langle m, \langle r \cdot 0, r \cdot 1, \cdots, r \cdot (m-1) \rangle \rangle \qquad (6.69)$$

$$\equiv \alpha W \circ distl : \langle m, svMpy : \langle r, iota : m \rangle \rangle \qquad (6.70)$$

$$\cong \alpha W \circ distl \circ [M\,, svMpy \circ [r\,, iota \circ M]] \quad \blacksquare \tag{6.71}$$

Theorem 2b:
$odds \circ H' \equiv svMpy \circ [W \circ [N, r]\,, \alpha W \circ distl \circ [M\,, svMpy \circ [r\,, iota \circ M]].$

Proof:

$$odds \circ H' \equiv odds \circ \alpha W \circ distl \circ [\times \circ [\bar{2}, M]\,, svMpy \circ [r\,, iota \circ \times \circ [\bar{2}, M]]] \tag{6.72}$$

$$\equiv \alpha W \circ odds \circ distl \circ [\times \circ [\bar{2}, M]\,, svMpy \circ [r\,, iota \circ \times \circ [\bar{2}, M]]] \tag{6.73}$$

But by Lemma 4b,

$$odds \circ distl \equiv distl \circ [1, odds \circ 2]. \tag{6.74}$$

So $odds \circ H'$

$$\equiv \alpha W \circ distl \circ [1, odds \circ 2] \circ [\times \circ [\bar{2}, M]\,, svMpy \circ [r\,, iota \circ \times \circ [\bar{2}, M]]] \tag{6.75}$$

$$\equiv \alpha W \circ distl \circ [\times \circ [\bar{2}, M]\,, odds \circ svMpy \circ [r\,, iota \circ \times \circ [\bar{2}, M]]] \tag{6.76}$$

Applying Lemma 4b again, and, using the definition of *svMpy*:

$$\equiv \alpha W \circ distl \circ [\times \circ [\bar{2}, M]\,, svMpy \circ [r\,, odds \circ iota \circ \times \circ [\bar{2}, M]]] \tag{6.77}$$

By Lemma 1b:

$$\equiv \alpha W \circ distl \circ [\times \circ [\bar{2}, M]\,, svMpy \circ [r\,, \alpha(add1 \circ multBy2) \circ iota \circ M]] \tag{6.78}$$

$$\cong \alpha W \circ distl : \langle 2m\,, svMpy : \langle r\,, \langle 1+2\cdot 0, 1+2\cdot 1, \,.\,.\,.\,.\,, 1+2\cdot(m-1)\rangle\rangle\rangle \tag{6.79}$$

$$\equiv \alpha W \circ distl : \langle 2m\,, \langle r(1+2\cdot 0), r(1+2\cdot 1), \,.\,.\,.\,.\,, r(1+2\cdot(m-1))\rangle\rangle \tag{6.80}$$

$$\equiv \alpha W \circ distl : \langle 2m\,, \langle (2r\cdot 0+r), (2r\cdot 1+r), \,.\,.\,.\,.\,, (2r\cdot(m-1)+r)\rangle\rangle \tag{6.81}$$

$$\equiv \langle W : \langle 2m, (2r\cdot 0+r)\rangle,\ W : \langle 2m, (2r\cdot 1+r)\rangle,\ \cdots\,,\ W : \langle 2m, (2r\cdot(m-1)+r)\rangle\rangle \tag{6.82}$$

But

$$W : \langle 2m, 2rk+r\rangle \equiv \times : \langle W : \langle n, r\rangle,\ W : \langle m, rk\rangle\rangle \tag{6.83}$$

e.g.

$$W_{2M}^{(2rk+r)} \equiv W_N^r \times W_M^{rk} \tag{6.84}$$

So (6.82) simplifies to:

$$svMpy : \langle W : \langle n, r\rangle, \langle W : \langle m, r\cdot 0\rangle,\ W : \langle m, r\cdot 1\rangle,\ \cdots\,,\ W : \langle m, r\cdot(m-1)\rangle\rangle\rangle \tag{6.85}$$

$$\equiv svMpy : \langle W : \langle n, r\rangle,\ \alpha W \circ distl : \langle m\,, \langle r\cdot 0\,, r\cdot 1 \cdots\,, r\cdot(m-1)\rangle\rangle\rangle \tag{6.86}$$

$$\equiv svMpy : \langle W : \langle n, r\rangle,\ \alpha W \circ distl : \langle m\,, svMpy : \langle r\,, \langle 0\,, 1 \cdots\,, (m-1)\rangle\rangle\rangle\rangle \tag{6.87}$$

$$\equiv svMpy : \langle W : \langle n, r\rangle,\ \alpha W \circ distl : \langle m\,, svMpy : \langle r\,, iota : m\rangle\rangle\rangle \tag{6.88}$$

$$\cong svMpy \circ [W \circ [N, r]\,, \alpha W \circ distl \circ [M, svMpy \circ [r, iota \circ M]]] \quad \blacksquare \tag{6.89}$$