ACM APL *Quote Quad* **23**, 2 (December 1992), 27-31.

On the Permutations of a Vector Obtainable through the Restructure and Transpose Operators of APL

Henry G. Baker, Jr.

1974-1975

University of Pennsylvania Computer Science Dept. and M.I.T. Computer Science Dept.

Abstract

Many times in the course of solving a problem in APL it becomes necessary to transpose an array in conjunction with restructuring. The interpretation of a two-dimensional matrix as a *block matrix*, i.e., a matrix of matrices, which in APL could be modelled as a four-dimensional array, is such a case. This paper presents many propositions which should help the APL user form a better understanding of the transpose operation in conjunction with the row-major representation which APL uses for matrices.

Contributions of this paper include the concepts of *partial ravel* and *refinement* of arrays, the collapsing of chains of transposes and restructures, and a theorem characterizing the cycle structure of the permutation of a vector induced by a two-dimensional transpose operation. The solution to the block matrix problem is included as an appendix.

Introduction

This paper consists of 4 parts. The first part considers the restructure operator alone; the second, the transpose operator alone; the third, both together; and an appendix which presents the actual block matrix transforms.

We assume complete familiarity with the APL language and use its notation throughout.[1] We also use a metalanguage predicate "x≡y" which asserts that the APL expressions x and y both evaluate to the same APL object. Proofs will be very sketchy, and omitted where trivial.

Restructure

Definition. Let A be an APL array. Then S←ρA is its *shape* and D←×\ρA is its *outline*.

Proposition 1. The shape S of an array can be reconstructed from its outline D.

Proof: S←D÷1,(-1)↓D. QED

Definition. Consider an array A. If S is a vector of positive integers, then SρA is a *conservative* restructure of A if and only if (×/S) ≡ (×/ρA).

This definition is motivated by the following proposition:

Proposition 2. A restructuring S of an array A preserves the ravel of A if and only if it is conservative; i.e. (,A) ≡ (,SρA).

We consider only conservative restructuring operations because we are interested in *permutations* of a vector. Any non-conservative restructuring will either copy or lose elements of the array. However, even some conservative restructurings seem to violate the meaning of an array; for example, suppose A were a 6×4 matrix. If we were to restructure it as a 4×6 matrix, *without first transposing it*, this would seem to destroy the integrity of the rows and columns and lend credence to the belief that the original data had no such inherent two-dimensional structure. However, in many cases it *would* be reasonable to restructure it as a 3×2×4 array, a 6×2×2 array, or a 24 element

[1]Due to the lack of an APL character set, we use ∅ for APL 'transpose' and ∆ for APL 'grade up'.

vector in order to make finer or coarser distinctions of the same type as block matrices. These comments motivate the next few definitions.

Definition. A vector V is a *compression* of the vector W if and only if there exists a boolean vector B such that V ≡ (B/W). If SρA is a conservative restructure of A and its outline (×\S) is a compression of the outline (×\ρA) of A, then SρA will be called a *partial ravel* of A.

Example: If (ρA) ≡ 3 5 7, then 3 35ρA; 15 7ρA; and 105ρA are all partial ravels of A because 3 105; 15 105; and 105 are all compressions of 3 15 105. However, 5 3 7ρA is not a partial ravel of A because 5 15 105 is not a compression of 3 15 105.

I contend that partial ravels are the only meaningful re-interpretations of A as an array of the same or lower dimension (APL *rank*). A is itself a partial ravel of A; (,A) is also a partial ravel of A.

Proposition 3. Partial ravel is a partial ordering of the set of partial ravels of an array A.

Definition. If B and C are both partial ravels of A, with outlines D and E, respectively, then the outline of B∩C is the longest compression of both D and E and the outline of B∪C is the shortest compression of the outline of A which has both D and E as compressions. From the outline and A itself, the arrays B∩C and B∪C can be constructed.

Proposition 4. The set of partial ravels of A forms a complete lattice under ∩,∪ with bottom element (,A) and top element A.

Definition. A restructure SρA of an array will be called a *refinement* of A if and only if A is a partial ravel of SρA.

Example: If (ρA) ≡ 3 6, then 3 2 3ρA is a refinement of A.

There are trivial refinements which are generated by inserting 1's into ρA like 1 3 6ρA where (ρA) ≡ 3 6. Since transposing these trivial coordinates will not move any elements, we consider only arrays without trivial coordinates.

Definition. An array A will be called *regular* if and only if ~1∊ρA.

We will henceforth be concerned only with regular arrays.

Proposition 5. If B,C are regular partial ravels of the regular array A with outlines D,E,F respectively, then the outlines B∩C and B∪C can be computed by (D∊E)/D and ((F∊D)∨(F∊E))/F, respectively.

Definition. An array A will be called *simple* if and only if it has no nontrivial regular refinements.

Proposition 6. A regular array A is simple if and only if every element n∊ρA is a prime integer.

Definition. An *alias* of a regular array A is either a regular refinement or a partial ravel of A.

Proposition 7. The set of aliases of a regular array A forms a lower semilattice under the ∩ operation.

Corollary. The set of aliases of a simple regular array forms a complete lattice.

We have thus completely characterized the arrays generated from a given array by "reasonable" restructures. In particular, any chain of conservative restructures can be collapsed to one—the last.

Transposes

The transpose operator of APL, when supplied with a permutation of the coordinates of an array, acts on the array in such a way that the coordinates are variously interchanged. The effect is to induce a permutation on the ravel of the array. The set of permutations of the coordinates of an array is obviously the symmetric group on the m coordinates under the group operation of permutation composition, where m is the dimension (APL "rank") of the array; i.e., m ≡ ρρA.

<u>Proposition 8</u> (Prop. TR10 of [Abrams70]). The transpose operator induces a homomorphism from the symmetric group of the coordinates into the symmetric group of the ravelled array.

Proof: $(P\varnothing Q\varnothing A) \equiv (P[Q])\varnothing A$, where P,Q are permutations of $\iota\rho\rho A$. QED

<u>Corollary</u>. The inverse of $P\varnothing$ is $(\Delta P)\varnothing$.

Proof:

$$(\Delta P)\varnothing P\varnothing A \equiv ((\Delta P)[P])\varnothing A \equiv (\iota\rho\rho A)\varnothing A \equiv A.$$
$$P\varnothing(\Delta P)\varnothing A \equiv (P[\Delta P])\varnothing A = (\iota\rho\rho A)\varnothing A = A.$$

QED

<u>Corollary</u>. Any chain of transposes can be collapsed into one transpose.

<u>Proposition 9</u>. $(\rho P\varnothing A) \equiv (\rho A)[P]$.

Transposes and Restructures

We now consider the transpose and restructure operators together.

<u>Proposition 10</u>. Any chain of transposes and conservative restructures can be collapsed so that transposes and restructures alternate.

Proof: Follows from Prop. 3 and corollary to Prop. 8. QED

<u>Proposition 11</u>. The permutation induced by any transpose of an array A can also be induced as a transpose of any refinement of A.

<u>Example</u>: The vector $(,2\ 1\varnothing 4\ 2\rho\iota 8)$ is the same as the vector $(,3\ 1\ 2\varnothing 2\ 2\ 2\rho\iota 8)$.

This proposition can also be turned around.

Definition. A vector P of integers is said to have a *consecutive subsequence* if $P[m,m+1] = n,n+1$ for some m,n.

<u>Corollary</u>. The permutation induced by any transposition $P\varnothing A$ of an array A in which P has a consecutive subsequence can always be induced by a transpose of a proper partial ravel of A.

<u>Example</u>: In the previous example, 1 2 is a consecutive subsequence of 3 1 2.

<u>Corollary</u>. Every induced permutation of an array A is an induced permutation of a simple regular refinement of A.

<u>Proposition 12</u>. The inverse of $P\varnothing S\rho$ is $(\rho A)\rho(\Delta P)\varnothing$; the inverse of $S\rho P\varnothing$ is $(\Delta P)\varnothing((\rho A)[P])\rho$, where A is the intended operand.

Proof:

$$\begin{aligned}
&(\rho A)\rho(\Delta P)\varnothing P\varnothing S\rho A \\
&\equiv (\rho A)\rho((\Delta P)[P])\varnothing S\rho A \\
&\equiv (\rho A)\rho(\iota\rho P)\varnothing S\rho A \\
&\equiv (\rho A)\rho S\rho A \\
&\equiv A \\
&(\Delta P)\varnothing((\rho A)[P])\rho S\rho P\varnothing A \\
&\equiv (\Delta P)\varnothing((\rho A)[P])\rho P\varnothing A \\
&\equiv (\Delta P)\varnothing P\varnothing A \\
&\equiv ((\Delta P)[P])\varnothing A \\
&\equiv (\iota\rho P)\varnothing A \\
&\equiv A
\end{aligned}$$

QED

<u>Proposition 13</u>. Every chain of transposes and refinements can be collapsed into one refinement followed by one transposition.

Proof: Follows from Prop. 11 and corollary to Prop. 8. QED

<u>Proposition 14</u>. Every chain of transposes and partial ravels can be collapsed into one transpose followed by one partial ravel.

Definition. The *induced group* of a vector V is the group of permutations of V generated by chains of transposes and conservative restructures of V.

Proposition 15. The induced group of a vector whose length is p^n, for some prime p and some positive integer n, is isomorphic to S_n, the symmetric group on n elements.

Proof: The vector V has but one simple regular refinement, (nρp)ρV, all induced permutations of V are induced by transpositions of this refinement, thus the induced group is an image of S_n. Since some element is always moved by a non-identity transposition, the kernel of the homomorphism is trivial, therefore it is an isomorphism. QED

Proposition 16. The induced group of a vector whose length is pq, where p,q are distinct primes, is cyclic.

Proof: The only simple refinements are (p,q)ρ and (q,p)ρ whose non-trivial transposes are inverse permutations of each other. Since the group is generated by one element, it is cyclic. QED

We now take up in detail the cycle structure induced by two-dimensional transposes, a problem investigated in [Pall60] and [Brenner73]. Additional background may be found in [Bolker70].

Definition. If n is a positive integer, let Φ(n) be the set of positive integers ≤n which are relatively prime to n. The size of Φ(n) is ϕ(n), which is Euler's totient function. Let (m,n) denote the greatest common divisor of m and n.

Proposition 17. Φ(n) is a multiplicative group modulo n.

Definition. If x∈Φ(n), then the *order* of x is the least positive integer r such that $x^r \equiv 1$ (mod n). If P is a permutation, then the *order* of P is the number of times P must be applied to put everything back in its original order.

Example: Using 0-origin indexing, ∅3 5ρι15 is 0 5 10 1 6 11 2 7 12 3 8 13 4 9 14 giving the cycle structure: (0)(1 5 11 13 9 3)(2 10 8 12 4 6)(7)(14). The order of this permutation is obviously 6=ϕ(14).

Theorem. The order of the permutation of the vector V of length pq, where p,q are positive integers, induced by ,∅(p,q)ρV is equal to the order of p in Φ(pq-1).

Let m=pq-1.

Lemma 1 [Pall and Seiden, 1960]. Using 0-origin indexing, the element at position n of V is moved to position m|n×p in ,∅(p,q)ρV.

Proof: n=aq+b for some a,b. Therefore np = aqp+bp ≡ bp+a (mod pq-1). But bp+a is the transposed position. QED

Lemma 2 [Pall and Seiden, 1960]. The subcycle of the induced permutation starting with j is generated by jp^r (mod m), r=1,2,3,...

Lemma 3. The length of the subcycle starting with j is the order of p in Φ(n') where m'=m/(m,j).

Proof: To solve $jp^r \equiv j$ (mod m), we must divide common factors to get $j'p^r \equiv j'$ (mod m'), where j'=j/(m,j) and m'=m/(m,j). Since (j',m')=1, j' has an inverse in Φ(m') so $p^r \equiv 1$ (mod m'). But this is the definition of the order of p in Φ(m'). QED

Lemma 4. The length of the subcycle starting with j divides the length of the subcycle starting with 1.

Proof: If $p^r \equiv 1$ (mod m), then $p^r \equiv 1$ (mod m') for any m' which divides m because $p^r = 1+mc+1+m'dc \equiv 1$ (mod m'). Therefore if $p^r \equiv 1$ (mod m) and $p^s \equiv 1$ (mod m'), then s≤r. Assume s is the least non-negative integer such that $p^s \equiv 1$ (mod m'). Then r=sf+t for some f, t<s. But $1 \equiv p^r = p^{sf+t} = (p^s)^f p^t \equiv p^t$ (mod m'). Therefore t=0 and s divides r. QED

Proof of Theorem: The order of the induced permutation is the least common multiple of the lengths of its subcycles. Since the length of every subcycle divides the length of the subcycle starting with 1, the order of the induced permutation is the same as the length of that subcycle, i.e., the order of p in Φ(m). QED

Corollary. The order of the induced permutation divides φ(m) and is equal only if p is a primitive root of m=pq-1.

Corollary. The order of the induced permutation is as big as pq-2 only when pq-1 is prime. This requires that either p or q is divisible by 2.

These last few theorems should be of some use in finding good algorithms for transposing matrices in place (see [Brenner73]).

Appendix: Block Matrices

We can now solve the problem of block matrices.

Given an m×nw matrix A, interpret it as an m×n matrix of w-element vectors.

(1) (m,n,w)ρA

Given an ml×n matrix A, interpret it as an m×n matrix of l-element column vectors.

(2) 2 1 3⌽(n,m,l)ρ2 1⌽A ≡ 1 3 2⌽(m,l,n)ρA

Given an ml×nw matrix A, interpret it as an m×n matrix of l×w matrices.

(3) 2 1 3 4⌽(n,m,l,w)ρ2 1 3⌽(ml,n,w)ρA ≡ 1 3 2 4⌽(m,l,n,w)ρA

Given an m×n matrix of l×w matrices, interpret it as a ml×nw matrix.

(4) (ml,nw)ρ1 3 2 4⌽A

Given an m×n matrix of numbers, expand to an m×n×l×w matrix by copying.

(5) 3 4 1 2ρ(l,w,m,n)ρA

Given an m×n matrix of numbers, expand to an ml×nw matrix by copying.

(6) (ml,nw)ρ1 3 2 4⌽3 4 1 2⌽(l,w,m,n)ρA ≡ (ml,nw)ρ2 4 1 3⌽(l,w,m,n)ρA

These operations can be quite profitably used in picture processing.

References

Abrams, P. An APL Machine. SLAC Report 114, Stanford U., Stanford, Cal., February, 1970.
Bolker, E. *An Introduction to Number Theory, An Algebraic Approach*. Benjamin, N.Y., 1970.
Brenner, N. Matrix transpose in place. Algorithm 467, *CACM 16*, 11 (1973), 692-4.
Pall, G., and Seiden, E. A Problem in Abelian Groups with Applications. *Math. Comp. 14* (1960), 189-192.

