Appendix D

Michelle Bodnar, Andrew Lohr

April 12, 2016

Exercise D.1-1

Let $C = A + B$ and $D = A - B$. Then, since A and B are symmetric, we know that $a_{ij} = a_{ji}$ and $b_{ij} = b_{ji}$. We consider these two matrices C and D now.

$$\begin{aligned} c_{ij} &= a_{ij} + b_{ij} \\ &= a_{ji} + b_{ji} \\ &= c_{ji} \end{aligned}$$

$$\begin{aligned} d_{ij} &= a_{ij} - b_{ij} \\ &= a_{ji} - b_{ji} \\ &= d_{ji} \end{aligned}$$

Exercise D.1-2

From the definitions of transpose and matrix multiplication we have

$$\begin{aligned} (AB)^T_{ij} &= (AB)_{ji} \\ &= \sum_{k=1}^{n} a_{jk} b_{ki} \\ &= \sum_{k=1}^{n} b_{ki} a_{jk} \\ &= (B^T A^T)_{ij}. \end{aligned}$$

Therefore $(AB)^T = B^T A^T$. This implies $(A^T A)^T = A^T (A^T)^T = A^T A$, so $A^T A$ is symmetric.

Exercise D.1-3

Suppose that A and B are lower triangular, and let $C = AB$. Being lower triangular, we know that for $i < j$, $a_{ij} = b_{ij} = 0$. To see that C is lower triangular,

$$\begin{aligned}
c_{ij} &= \sum_{k=1}^{n} a_{ik}b_{kj} \\
&= \sum_{k=1}^{j-1} a_{ik}b_{kj} + \sum_{k=j}^{n} a_{ik}b_{kj} \\
&= \sum_{k=1}^{j-1} a_{ik}0 + \sum_{k=j}^{n} 0b_{kj} \\
&= \sum_{k=1}^{j-1} 0 + \sum_{k=j}^{n} 0 \\
&= 0 + 0 = 0
\end{aligned}$$

Exercise D.1-4

Suppose row i of P has a 1 in column j. Then row i of PA is row j of A, so PA permutes the rows. On the other hand, column j of AP is column i of A, so AP permutes the columns. We can view the product of two permutation matrices as one permutation matrix permuting the rows of another. This preserves the property that there is only a single 1 in each row and column, so the product is also a permutation matrix.

Exercise D.2-1

$$\begin{aligned}
I &= I \\
AC &= AB \\
B(AC) &= B(AB) \\
(BA)C &= (BA)B \\
IC &= IB \\
C &= B
\end{aligned}$$

Exercise D.2-2

Let L be a lower triangular matrix. We'll prove by induction on the size of the matrix that the determinant is the product of its diagonal entries. For $n = 1$, the determinant is just equal to the matrix entry, which is the product of the only diagonal element. Now suppose the claim holds for n, and let L be $(n+1) \times (n+1)$. Let L' be the $n \times n$ submatrix obtained from L by deleting the first row and column. Then we have $\det(L) = L_{11}\det(L')$, since $L_{1j} = 0$ for all $j \neq 1$. By the induction hypothesis, $\det(L')$ is the product of the diagonal entries of L', which are all the diagonal entries of L except L_{11}. The claim follows since we multiply this by L_{11}.

We will prove that the inverse of a lower triangular matrix is lower triangular by induction on the size of the matrix. For $n = 1$ every matrix is lower triangular, so the claim holds. Let L be $(n+1)\times(n+1)$ and let L' be the submatrix obtained from L by deleting the first row and column. By our induction hypothesis, L' has an inverse which is lower triangular, call it L'^{-1}. We will construct a lower triangular inverse for L:

$$L^{-1} = \left[\begin{array}{c|ccc} 1/l_{11} & 0 & \cdots & 0 \\ \hline a_1 & & & \\ \vdots & & L'^{-1} & \\ a_n & & & \end{array}\right]$$

where we define a_i recursively by

$$a_1 = -L_{21}/(L_{11}L'_{11}) \text{ and } a_i = -\left(L_{(i+1),1}/L_{11} + \sum_{k=1}^{i-1} L'_{ik}a_k\right)/L'_{ii}.$$

It is straightforward to verify that this in fact gives an inverse, and it is well-defined because L is nonsingular, so $L_{ii} \neq 0$.

Exercise D.2-3

We will show that it is invertible by showing that P^T is its inverse. Suppose that the only nonzero entry of row i is a one in column $\sigma(i)$. This means that the only nonzero entry in column i of P^T is in row $\sigma(i)$. If we let $C = PP^T$, then, for every i and j, we have that $c_{ij} = \sum_{k=1}^n p_{ik}p_{jk} = p_{i\sigma(i)}p_{j\sigma(i)}$. Since σ is a bijection, we have that if $i \neq j$, then $\sigma(i) \neq \sigma(j)$. This means that $c_{ij} = 0$. However, if $i = j$, then $c_{ij} = 1$. That is, their product is the identity matrix. This means that P^T is the inverse of P.

Since a permutation matrix is defined as having exactly one one in each row and column, we know that this is true of P. However, the set of rows of P^T is the set of columns of P, and the set of columns of P^T are the set of rows of P. Since all of those have exactly one one, we have that P^T is a permutation matrix.

Exercise D.2-4

Assume first that $j \neq i$. Let C_{ij} be the matrix with a 1 in position (i,j), and zeros elsewhere, and $C = I + C_{ij}$. Then $A' = CA$, so $A'^{-1} = A^{-1}C^{-1}$. It is easy to check that $C^{-1} = I - C_{ij}$. Moreover, right multiplication by C^{-1} amounts to subtracting column i from column j, so the claim follows. The claim fails to hold when $i = j$. To see this, consider the case where $A = B = I$. Then A' is invertible, but if we subtract column i from column j of B we get a matrix with a column of zeros, which is singular, so it cannot possibly be the inverse of a matrix.

Exercise D.2-5

To see that the inverse of a matrix that has only real entries must be real. Imagine instead that that matrix was a matrix over $\mathbb{R}$. Then, it will have a inverse in this ring of matrices so long as it is non-singular. This inverse will also be an inverse of the matrix when viewed as a matrix of $\mathbb{C}$. Since inverses are distinct, this must be its inverse, and is all real entries because it was originally computed as a matrix that was in the set of real entry matrices.

To see the converse implication, just swap the roles, computing the inverse of the inverse. This will be the original matrix.

Exercise D.2-6

We have $(A^{-1})^T = (A^T)^{-1} = A^{-1}$ so A^{-1} is symmetric, and $(BAB^T)^T = (B^T)^T A^T B^T = BAB^T$.

Exercise D.2-5

We will consider the contrapositive. That is, we will show that a matrix has rank less than n if and only if there exists a null vector.

Suppose that v is a null vector, and let $a_1, a_2, \dots a_n$ be the columns of A. Since multiplying a matrix by a vector produces a linear combination of its columns whoose coefficients are determined by the vector v that we are multiplying by. Since v evaluates to zero, we have just found a linear combination of the set of columns of A that sums to zero. That is, the columns of A are linearly dependent, so the column rank is less than n, since the set of all vectors is not linearly independent, the largest independent set must be a proper subset.

Now, suppose that the column rank is less than n. This means that there is some set of column vectors which are linearly dependent. Let v_i be the coefficient given to the ith column of A in this linear combination that sums to zero. Then, the v_i values combine into a null vector.

Exercise D.2-8

Let A be $m \times p$ and B be $p \times n$. Recall that rank(AB) is equal to the minimum r such that there exist F and G of dimensions $m \times r$ and $r \times n$ such that $FG = AB$. Let A' and A'' be matrices of minimum r' such that $A'A'' = A$ and the dimensions are $m \times r'$ and $r' \times p$. Let B' and B'' be the corresponding matrices for B, which minimize r''. If $r' \leq r''$ we have $A'(A''B'B'') = AB$, so $r \leq r'$ since r was minimal. If $r'' \leq r'$ we have $(A'A''B')B'' = AB$, so $r \leq r''$, since r was minimal. Either way, $\text{rank}(AB) \leq \min(\text{rank}(A), \text{rank}(B))$.

The product of a nonsingular matrix and another matrix preserves the rank of the other matrix. Since the rank of a nonsingular $n \times n$ matrix is n and the rank of an $m \times n$ or $n \times m$ matrix is bounded above by $\min(m, n)$, the rank of

AB is bounded above by the minimum of n and the rank of the other matrix, which is the minimum of the rank of each of the matrices.

Problem D-1

We'll proceed by induction on n. If $n = 1$, then, the matrix is just the 1×1 matrix with it's only entry 1. This clearly has a determinant of 1. Also, since there is no way to pick distinct i and j in the product on the right hand side, the product is just one as well.

Now, suppose it is true for $n \times n$ Vandermonde matrices, we will show it for $(n + 1) \times (n + 1)$ Vandermonde matrices. Now, suppose that we, as the hint suggests, starting at the second from rightmost column and working left, add $(-x_0)$ times that column to the one to its right. Since the determinant is unaffected by this sort of operation,we won't be changing the determinant. For every entry in the top row except the leftmost one, we have made it zero, since it becomes $x_0^{j-1} - x_0^{j-2} \cdot x_0 = 0$. This means that we can do a expansion by minors along the top row to compute the determinant. The only nonzero term in this is the top left column. This means that the determinant is the same as the determinant of that one minor. Everything in the ith row of that minor has a factor of $(x_i - x_0)$. This means that if we take all those factors out, we have $\prod_{i=1}^{n-1}(x_i - x_0)$, which are all the factors in the formula that include x_0. Once we take that factors out, we are left with a $n \times n$ Vandermonde matrix on the variables $x_1, \ldots, x_{n-1}$. So, we know that it will contain all the other factors we need to get the right hand side, completing the induction.

Problem D-2

a. Without loss of generality we may assume that the first r columns of A are linearly independent. Then for x_1 and $x_2 \in S_n$ such that x_1 and x_2 are not identical in the first r entries and have 0's in the remaining entries we have that $Ax_1 \neq Ax_2$. This is because the first r entries of each are a linear combination of the first r rows of A, and since they are independent there can't be two different linear combinations of them which are equal. Since there are at least 2^r non-equivalent vectors $x \in S_n$, we must have $|R(A)| \geq 2^r$. On the other hand, x is a vector which doesn't have 0's in the coordinates greater than r. Then $Ax = \sum_{x_i} a_i$ where a_i is the i^{th} column of A. Since each of the last $n - r$ columns of A is in fact a linear combination of the first r columns of A, this can be rewritten as a linear combination of the first r columns of A. Since we have already counted all of these, $|R(A)| = 2^r$. If A doesn't have full rank then the range can't include all 2^n elements of S_n, so A can't possibly define a permutation.

b. Let $y \in R(A)$ and $x_r, x_{r+1}, \ldots, x_{n-1}$ be arbitrary. Set $z = \sum_{i=r}^{n-1} a_i x_i$. Since the first i columns of A span the range of A and z is in the range of A, $y - z$ is in the range of A and there exist $x_0, x_1, \ldots, x_{r-1}$ such that $\sum_{i=0}^{r-1} a_i x_i = y - z$. Then we have $Ax = y - z + z = y$. Since the last $n - r$ entries of x were arbitrary, $|P(A, y)| \geq 2^{n-r}$. On the other hand, there are 2^r elements in $R(A)$, each with at least 2^{n-r} preimages, which means there are at least $2^r \cdot 2^{n-r} = 2^n$ preimages in total. Since $|S_n| = 2^n$, there must be exactly 2^{n-r} preimages for each element of the range.

c. First observe that $|B(S', m)|$ is just the number of blocks which contain an element of the range of S. Since the first m rows of A only affect the first m positions of Ax, they can affect the value of Ax by at most $2^m - 1$, which won't change the block. Thus, we need only consider the last $n - m$ rows. Without loss of generality, we may assume that S consists of the first block of S_n, so that only the first m columns of A are relevant. Suppose that the lower left $(n - m) \times m$ submatrix of A has rank r. Then the range of Ax consists of vectors of the form $[*, \cdots, *, x_0, x_1, \cdots x_{r-1}, 0, \cdots, 0]^T$, where there are m $*$'s. There are 2^{m+r} such vectors, spanning 2^r blocks. Thus, $|B(S', m)| = 2^r$. Since it is only the choice of $x_0, \ldots, x_{r-1}$ which determines the block we're in, and we can pick every possible combination, every block must be hit the same number of times. Thus, the number of numbers in S which map to a particular block is $2^m/2^r = 2^{m-r}$.

d. The number of linear permutations is bounded above by the number of pairs (A, c) where A is an $n \times n$ matrix with entries in $GF(2)$ and c is an n-bit vector. There are 2^{n^2+n} of these. On the other hand, there are $(2^n)!$ permutations of S_n. For $n \geq 3$, $2^{n^2+n} \leq (2^n)!$.

e. Let $n = 3$ and consider the permutation $\pi(0) = 0$, $\pi(1) = 1$, $\pi(2) = 2$, $\pi(3) = 3$, $\pi(4) = 5$, $\pi(5) = 4$, $\pi(6) = 6$ and $\pi(7) = 7$. Since $A \cdot 0 + c = 0$ we must have c be the zero vector. In order for $\pi(1)$ to equal 1, the first column of A must be $[1\ 0\ 0]^T$. To have $\pi(2) = 2$, the second column of A must be $[0\ 1\ 0]^T$. To have $\pi(3) = 3$, the third column of A must be $[0\ 0\ 1]^T$. This completely determines A as the identity matrix, making it impossible for $\pi(4) = 5$, so the permutation is not achievable by any linear permutation.