CoCoNuT Assignment Five

February 27, 2015

1 More Sage

Vector Commands

Caution: First entry of a vector is numbered zero.

```
sage: u = vector(QQ, [1, 3/2, -1])          # length 3 over rationals
sage: v = vector(QQ, {2:4, 95:4, 210:0})    # 211 entries, nonzero in entry 2 and entry 95, sparse
sage: v[0]
0
sage: v[2]
4
sage: w = vector(GF(3), 4,[1, 2, 0,1])      # vector over GF(3) of length 4
sage: u = vector(QQ, [1, 3/2, -1])
sage: v = vector(ZZ, [1, 8, -2])
2*u - 3*v                                   # linear combination
(-1,-21,4)
sage: u.dot_product(v)
15
sage: u.cross_product(v)                    # order: u*v
(-1,-21,4)
```

Matrix Commands

```
A = matrix(ZZ, [[1,2],[3,4],[5,6]])           # 3x2 over the integers
B = matrix(QQ, 2, [1,2,3,4,5,6])              # 2 rows from a list, so 2 * 3 over rationals
C = matrix(CDF, 2, 2, [[5*I, 4*I], [I, 6]])  # complex entries, 53-bit precision
Z = matrix(QQ, 2, 2, 0)                       # zero matrix
D = matrix(QQ, 2, 2, 8)                       # diagonal entries all 8, other entries zero
E = block_matrix([[P,0],[1,R]])               # very flexible input
II = identity_matrix(5)                       # 5 * 5 identity matrix

u = vector(QQ, [1,2,3]), v = vector(QQ, [1,2])
A = matrix(QQ, [[1,2,3],[4,5,6]])
B = matrix(QQ, [[1,2],[3,4]])
u*A, A*v, B*A, B^6, B^(-3)                    # All possible
f(x)=x^2+5*x+3                                # Then f(B) is possible

M = MatrixSpace(QQ, 3, 4)                     # Is space of 3 x 4 matrices
A = M([1,2,3,4,5,6,7,8,9,10,11,12])           # Coerce list to element of M, a 3 x 4 matrix over QQ
M.basis()
```

```
M.dimension()
M.zero_matrix()

5*A+2*B                                      # linear combination
A.inverse(), A^(-1), ~A,
A.transpose()
A.restrict(V)                                # Restriction to invariant subspace V

A.rescale_row(i,a) a*(row i)                 # Changes the matrix 'in place'
A.add_multiple_of_row(i,j,a)                 # a*(row j) + row i
A.swap_rows(i,j)

A.rref()                                     # rref() PROMOTES MATRIX TO FRACTION FIELD
A.echelon_form(), A.echelonize()
A.pivots()                                   # Indices of columns spanning column space
A.pivot_rows()                               # Indices of rows spanning row space

A.rank(), A.right_nullity()
A.left_nullity() == A.nullity()
A.determinant() == A.det()
```

The following commands produce true/false depending on whether the matrix has the given property

```
.is_zero(); .is_symmetric(); .is_hermitian();
.is_square(); .is_orthogonal(); .is_unitary();
.is_scalar(); .is_singular(); .is_invertible();
.is_one(); .is_nilpotent(); .is_diagonalizable()
```

Vector Spaces

The following are properties of a vector space

```
V.dimension()
V.basis()
V.echelonized_basis()
V.has_user_basis()                 # With non-canonical basis
V.is_subspace(W)                   # True if W is a subspace of V
V.is_full()                        # Rank equals degree (as module)
```

To construct a vector space (or module if the coefficients are a ring) we can form the span

```
span([v1,v2,v3], QQ)
```

If U and W are subspaces of V we have the commands

```
V.quotient(W)             # Quotient of V by subspace W
V.intersection(W)         # Intersection of V and W
V.direct_sum(W)           # Direct sum of V and W
V.subspace([v1,v2,v3])    # Specify basis vectors in a list
G=V.basis_matrix()        # Return a matrix whose rows are a basis of V
```

In the following for a matrix A the objects returned are a vector space when the base ring is a field, and a module otherwise:

```
A.left_kernel() == A.kernel()        # And right_ too works
A.row_space() == A.row_module()
A.column_space() == A.column_module()
```

2 Assignment Five Questions

1. (a) Using the SAGE command hamming_weight(), write a simple SAGE function Dist() that given two vectors $\mathbf{x}, \mathbf{y}$ in $\mathbb{F}_q^n$, returns the Hamming distance between $\mathbf{x}$ and $\mathbf{y}$.

   (b) Using Dist(), write a function C_Dist() that computes the distance of a given code C by exhaustive search.

   (c) Let C be the code of length 15 defined as

   $$\{a_1(101010101011100) + a_2(011011011001101) \mid a_1, a_2 \in \mathbb{Z}_7\}.$$

   Produce Sage code which list all the distinct codewords of C.

(d) Use the function C_Dist() to find the distance of C. What is the error correction capability t of C?

2. (a) Using the function Dist() defined in 1., give a SAGE function C_Decode() that given a received vector $\mathbf{r} \in \mathbb{F}_q^n$ finds the closest codeword $\mathbf{c} \in C$ by exhaustive search.

(b) Given the code C of Problem 1, and the received vector $\mathbf{r}$, use the function C_Decode to correct, if possible, $\mathbf{r}_1 = (1,0,2,0,4,3,0,2,5,6,2,6,2,1,6)$, and $\mathbf{r}_2 = (5,2,3,0,3,6,4,6,3,0,4,3,3,0,6)$ to the closest codeword.

3. Use SAGE to generate a repetition code over GF(q) with length n and list all the codewords. Call this function RepetitionCode (it takes as input q and n). Fix $q = 3$ and $n = 11$, list all the codeword of Rep$(3, 11)$.

4. (a) Use SAGE to define a function IsLinear that tests if a given a code C is linear.

   (b) Is the repetition code of Problem 3 linear? And the code of Problem 1?

(c) Write a simple function that outputs the number of all linear codes of a given length over GF(q) and dimension k.

5. Let C be a code of length 25 and suppose a Binary Symmetric Channel (BSC) with $p = 0.99$.

(a) What is the probability that a codeword C is received correctly?

(b) For each $\mathbf{c} \in C$, what is the probability that $\mathbf{r}$ is received such that $\mathrm{d}(\mathbf{r}, \mathbf{c}) = 1$?

6. Let $C = \{100001000010000, 010011000001110, 001001001001001\}$. Find all the errors that can not be detected by C.

7. Consider the space $\{0, 1\}^{18}$ with Hamming distance. Compute the volume of a sphere with radius 2.

8. Consider the binary code of length 5 and minimum distance 2, such that all the codewords have even weight; and a binary channel that has probability $p = 0.9$ that a transmitted symbol is received correctly and a probability of $1 - p$ of producing an erasure (so a ϵ is received). What is the probability that a codeword transmitted over this channel is decoded correctly?