Matematiska Institutionen
KTH

Solutions to homework number 5 to SF2736, fall 2014.

Please, deliver this homework at latest on Monday, December 15, 2014. Provide both your name and your e-mail address with your solutions.

The homework must be delivered individually, and, in general, just hand-written notes are accepted. You are allowed to discuss the problems with your classmates, but you are not allowed to deliver a copy of the solution of another student.

1. (0.1p) Find the number of words that cannot be corrected by the 1-error-correcting code C defined by the parity-check matrix

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Give examples of words that does not belong to C but can be corrected to a word in C.

Solution. The null space of the given matrix has dimension $10-4$. Thus,

$$|C| = 2^6 = 64.$$

The number of words that can be corrected or belong to C are at distance at most one from a code word, that is, in a 1-sphere $\mathrm{S}_1(\bar{c})$ with center at a could word $\bar{c}$. As

$$|\mathrm{S}_1(\bar{c})| = 1 + \binom{10}{1} = 11,$$

we get the number of words that cannot be corrected is

$$2^{10} - 64 \cdot 11 = 1024 - 704 = 320.$$

Words that cannot be corrected belongs to solutions of the system

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_{10} \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix}$$

for some column which is not a column of the matrix. (The words 0110000000 and 1010000000 can be found as words that cannot be corrected.) Words that can be corrected are 1000000000, 0100000000. (There was probably a mis-formulation, should probably have been "words that cannot be corrected". It is easy to find words that can be corrected, words at distance 1 from code words are such code words.)

2. (0.2p) Find the number of distinct necklaces that you can produce with ten beans that are either black or white. The answer must be given as an integer.

Solution. We use the lemma of Burnside and get the following table for our calculations.

$\varphi \in G$	$\lvert\text{Fix}(\varphi)\rvert$
id.	2^{10}
$\psi = (1\ 2\ \ldots\ 10)$	2
$\psi^2 = (1\ 3\ \ldots\ 9)(2\ 4\ \ldots 10)$	2^2
ψ^3	2
ψ^4	2^2
$\psi^5 = (1\ 6)(2\ 7)(3\ 8)(4\ 9)(5\ 10)$	2^5
ψ^6	2^2
ψ^7	2
ψ^8	2^2
ψ^9	2
$(1\ 10)(2\ 9)(3\ 8)(4\ 7)(5\ 6)$	2^5
$(1\ 9)(10)(2\ 8)(3\ 7)(4\ 6)(5)$	2^6
$\vdots$	
$(1\ 2)(3\ 10)(4\ 9)(5\ 8)(6\ 7)$	2^5

The number of distinct colorings of the necklace is then

ANSWER:

$$\frac{1}{|G|}\sum_{\varphi\in G}|\text{Fix}(\varphi)| = \frac{1}{20}(2^{10} + 4\cdot 2 + 4\cdot 2^2 + 2^5 + 5\cdot 2^5 + 5\cdot 2^6) = 78.$$

3. (0.3p) Solve, by using the technique with generating functions, the recursion

$$a_n - a_{n-1} - 12a_{n-2} = n, \qquad n = 2, 3, \ldots,$$

where $a_0 = 1$ and $a_1 = 2$.

Solution. We multiply the given equation with x^n:

$$a_n x^n - x a_{n-1} x n - 1 - 12x^2 a_{n-2} x^{n-2} = n x^n.$$

Let $A(x) = \sum_{n=0}^{\infty} a_n x^n$. Summation of the equation above for $n = 2, 3, \ldots$ gives

$$A(x) - a_1 x - a_0 - x(A(x) - a_0) - 12x^2 A(x) = x\sum_{n=2}^{\infty} n x^{n-1}.$$

We differentiate

$$\frac{1}{(1-x)^2} = \mathrm{D}(\frac{1}{1-x}) = \mathrm{D}(\sum_{n=0}^{\infty} x^n) = \sum_{n=0}^{\infty} n x^{n-1}. \tag{1}$$

Hence,

$$x\sum_{n=2}^{\infty} n x^{n-1} = x(\frac{1}{(1-x)^2} - 1).$$

Now, $1 - x - 12x^2 = (1-4x)(1+3x)$, so

$$(1-4x)(1+3x)A(x) = x + 1 + x(\frac{1}{(1-x)^2} - 1),$$

and

$$A(x) = \frac{1}{(1-4x)(1+3x)} + \frac{x}{(1-4x)(1+3x)(1-x)^2}$$

Using any method of producing partial fractions then gives

$$A(x) = -\frac{1}{12}\frac{1}{(1-x)^2} - \frac{13}{144}\frac{1}{1-x} + \frac{39}{112}\frac{1}{1+3x} + \frac{52}{63}\frac{1}{1-4x}.$$

Finally, using Equation (1) and the equality

$$\frac{1}{1-ax} = \sum_{n=0}^{\infty} a^n x^n,$$

we get

ANSWER:

$$a_n = -\frac{1}{12}(n+1) - \frac{13}{144} + \frac{39}{112}(-3)^n + \frac{52}{63}4^n.$$

4. (0.4p) In the direct product $\mathbb{Z}_3^n = \mathbb{Z}_3 \times \cdots \times \mathbb{Z}_3$ of n copies of the ring $\mathbb{Z}_3$ we define the distance between two vectors, or words, $\bar{x} = x_1 \ldots x_n$ and $\bar{y} = y_1 \ldots y_n$ by

$$\mathrm{d}(\bar{x}, \bar{y}) = |\{i \mid x_i \neq y_i\}|.$$

Generalize the concept of linear 1-error-correcting binary codes to codes consisting of words of length n formed by using the elements in $\mathbb{Z}_3$ as "letters". Construct a linear 1-error-correcting code with as many words as possible in the direct product $\mathbb{Z}_3^7 = \mathbb{Z}_3 \times \cdots \times \mathbb{Z}_3$.

Solution. We define a linear 1-error-correcting code as a set C of ternary words with the property that any two words of C are at distance at least 3, and that C is a subspace of the direct product S of n copies of the ring $\mathbb{Z}_3$. As we can divide with non-zero elements in this ring we can regard S

as a vector space with scalars $\mathbb{Z}_3$. The linear code C can then be verified to be the null space of some matrix $\mathbf{H}$.

The size of C is then equal to $3^{n-\text{rank}(\mathbf{H})}$.

As minimum distance in C must be 3, none of the columns of $\mathbf{H}$ can be the zero-column, and no column is a multiple of another column. Thus the columns represent distinct 1-dimensional subspaces of $\mathbb{Z}_3^k$, where k is the number of rows of $\mathbf{H}$.

Now to the case $n = 7$. The fewer rows of $\mathbf{H}$, the more words. Thus some necessary trial-and-error search.

We try with $k = 2$. The vector space $\mathbb{Z}_3^2$, contains $3^2 - 1$ non-zero vectors, and a 1-dimension subspace contains 2. Thus there are less then 4 1-dimensional subspaces in case $k = 2$.

We try with $k = 3$. As $(2^3 - 1)/2 = 14$ there might be in total 14 non-parallel 1-dimensional subspaces. (In fact there are exactly 14 non-parallel 1-dimensional subspaces.) Further trial and error gives the matrix

$$\mathbf{H} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 2 & 1 & 1 & 0 \end{pmatrix}$$

(There are quite a few more feasible matrices, indeeed

$$14 \cdot 13 \cdot \cdots \cdot 8 \cdot 2^7 = 2214051840$$

possibilities for the matrix $\mathbf{H}$.)