Math 116
Homework 6 Solutions

I graded 4 of the problems: 4, 6, 9, 12.

Each problem is worth 3 points. A grade of 0 indicates no solution or a substantially wrong solution. A grade of 3 indicates a correct or nearly correct solution. Otherwise the grade given is 1 or 2 depending upon how much work was put in and how close the solution is to being correct. How neat and clear your solution is also affects the grade I give.

If you believe a problem was misgraded, or I made some addition or other error, please write a short note explaining the situation, attach it to your homework, and return it to me (either in person, in my mailbox, or under my office door). I'll take a look and return the homework in the next section.

The following are solutions to the homework problems (excepting problems whose solutions are in the back of the text) and additional comments for the problems I graded.

General Comments
The maximum number of points was 12. The high score was 10, the median was 6 and the mean was exactly 5.

2. The plaintext space and ciphertext space, and are both $\{\mathrm{A}, \ldots, \mathrm{Z}\}$, the same as for the Caeser cipher. They key space is now a set of pairs (k_1, k_2), where $k_1, k_2 \in \{\mathrm{A}, \ldots, \mathrm{Z}\}$. We need only describe the decryption algorithm, which uses the same pair of keys (k_1, k_2) as the encryption algorithm. It does the obvious thing: First reverse the string and then decrypt (as in the Caesar cipher) the odd-numbered elements with k_1 and the even-numbered elements with k_2.

   Note that this problem is quite poorly worded, and it isn't clear whether the author is talking about the encodings of the elements being odd or the positions of the elements being odd. However the latter is really the only interpretation that makes sense.

4. We need to handle two cases, for n even and odd. For n even, once the first $n/2$ components of the string are determined (and they can be arbitary), then the entire string is determined. So the number of such strings is $|\Sigma|^{n/2}$. For n odd the first $\frac{n+1}{2}$ components determine the entire string. So the number of such strings in this case is $|\Sigma|^{(n+1)/2}$. An answer which works for both cases is to say that the number of strings is $|\Sigma|^{\lceil n/2 \rceil}$.

6. For a given block length n, a block cipher over $\{0, 1\}$ is determined completely once the encryption function/key space is determined. If the number of ones is to be preserved, then the encryption function must be a bit permutation and the cipher a permutation cipher (page 78). As shown on page 76, there are $n!$ bit permutations for each length n, so that is the number of block ciphers for block length n.

   Prof. Blasius has informed me that this undercounts the number of distinct ciphers (at least for $n > 2$); there are some additional block ciphers that are not bit permutations. The correct way to count the number of ciphers is the following. Note that as the number of ones is to be preserved, the strings with exactly k ones must be permuted among themselves. Now there are $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ strings with exactly k ones, for $0 \leq k \leq n$. Since each such string can be sent to any other with the same number of ones, there are $\binom{n}{k}!$ permutations just of the subset of strings with exactly k ones. Now as each of these permutations is independent of the others, there are $\prod_{k=0}^{n} \binom{n}{k}!$ total ciphers.

   As I learned my own answer was incorrect after I graded the problems, I still gave full credit to those who answered $n!$ and explained their reasoning.

8. One can come up with all sorts of examples. One example would be a modified Caeser cipher in which the plaintext space is the set of letters $\{\mathrm{A}, \ldots, \mathrm{Z}\}$ (say encoded in ASCII), while the ciphertext space is the entire ASCII character set.

12. There are many possibilities. First note that if $f(\vec{v}) = A\vec{v} + \vec{b}$ is an affine linear transformation, then $f(\vec{0}) = \vec{b}$, where $\vec{0}$ is the vector of all zeros. So say $f(\vec{0}) = \vec{0}$ for simplicity; this forces the transformation to be linear. Now let $\vec{e_i}$ be the vector with 1 in the ith position and 0 everywhere else. Then the $\vec{e_i}$ are linearly independent for $1 \leq i \leq n$, and so A is determined completely by them; in fact the columns of A are exactly the $\vec{e_i}$. Again for simplicity say that each $\vec{e_i}$ maps to itself, so A is in fact the identity matrix. Then if the permutation is to be affine linear, it follows every vector must map to itself. However we are free to permute the remaining vectors however we like; any nonidentity permutation of them is a non-affine linear permutation.

    Notice that this strategy doesn't work for $n = 1$ or $n = 2$. In fact every permutation for $n = 1$ or $n = 2$ must be affine linear, as you can prove. However for $n \geq 3$ one can always find an permutation which is non-affine linear, as was shown above.

    Comments: Although this was just basic linear algebra, surprisingly no one got it right. In fact only one student got as much as one point out of three for the problem.

17. The determinant is $1(6-1) - 2(4-3) + 3(2-9) = 5 - 2 - 21 = -18$.

19. There are many possibilities. A simple is one is $f(\vec{v}) = I\vec{v} + \vec{b}$ where I is the 3×3 identity matrix and $\vec{b} = (1, 1, 1)^T$ (since we are in $\mathbb{Z}/2\mathbb{Z}$).