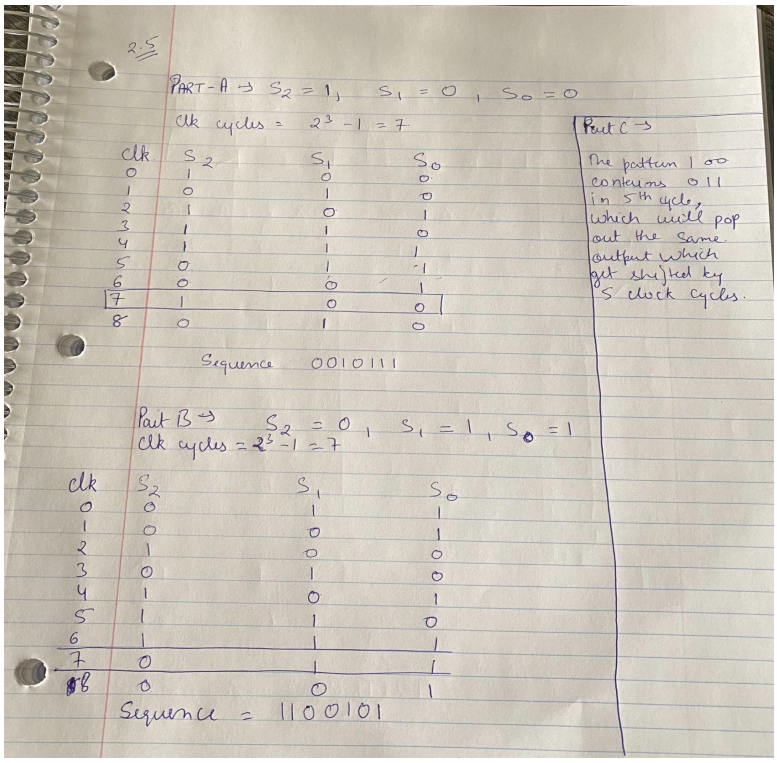
2.5. We will now analyze a pseudorandom number sequence generated by a LFSR characterized by ($c2 = 1$, $c1 = 0$, $c0 = 1$).
What is the sequence generated from the initialization vector ($s2 = 1$, $s1 = 0$, $s0 = 0$)?
What is the sequence generated from the initialization vector ($s2 = 0$, $s1 = 1$, $s0 = 1$)?
How are the two sequences related?



2.6. Assume we have a stream cipher whose period is quite short. We happen to know that the period is 150–200 bits in length. We assume that we do *not* know anything else about the internals of the stream cipher. In particular, we should not assume that it is a simple LFSR. For simplicity, assume that English text in ASCII format is being encrypted.

Describe in detail how such a cipher can be attacked. Specify exactly what Oscar has to know in terms of plaintext/ciphertext, and how he can decrypt all ciphertext.

Answer:
Assuming we have some plaintext and its cipher text, we can XOR the first 200 bits(or more) of the plaintext and ciphertext, to get the key and check to see when the key starts repeating between 150-200 bits. Then we can use this key to decipher the whole text and check if the deciphered text is legible english.

If it is, most likely our key is correct because we know that the text that was encrypted was English text.

If it is not, then we try with some other portion of bits for plaintext and its ciphertext.