Suggested Solutions.

1(a). $[n,k]$-code is a linear code of length n and dimension k

(b). $V(n,q)$ denotes the vector space of all length-n vectors with entries in $GF(q)$ (or the field with q elements)

2.(a). We know ISBN satisfies $\sum_{i=1}^{10} i x_i \equiv 0 \pmod{11}$

$$\therefore\ 1\cdot 2 + 2\cdot 8 + 3\cdot 4 + 4\cdot 2 + 5\cdot 4 + 6\cdot d + 7\cdot 0 + 8\cdot 1 + 9\cdot 0 + 10\cdot 8 \equiv 0 \pmod{11}$$

$$2 + 5 + 1 + 8 + 9 + 6d + 8 + 80 \equiv 0 \pmod{11}$$

$$6d + 3 \equiv 0 \pmod{11}$$

$$6d \equiv 8 \pmod{11}.$$

$$d \equiv 8 \times (6^{-1}) \pmod{11}$$

$$d \equiv 8 \times 2 \equiv 5 \pmod{11}.$$

$6^{-1} \equiv 2 \pmod{11}$ since $2 \times 6 \equiv 12 \equiv 1 \pmod{11}$.

(b) First observe that $37 \cdot 100 \equiv 3700 \equiv -1 \pmod{3701}$.

$$\Rightarrow\ (-37)\cdot 100 \equiv -(37\cdot 100) \equiv -(-1) \equiv 1 \pmod{3701}$$

$$\Rightarrow\ 100^{-1} \equiv -37 \equiv 3701 - 37 \equiv 3664 \pmod{3701}.$$

Alternatively, we want to find $\underline{x}$ s.t.

$$100\underline{x} \equiv 1 \pmod{3701}.$$

$$\Rightarrow\ 100\underline{x} = 3701k + 1 \qquad \text{for some } k \in \mathbb{Z}$$

Take $k = 99$ makes the last two digits of $(3701k+1)$ both zero.

$$\Rightarrow\ 100\underline{x} = 3701 \times 99 + 1$$

$$= (37 \times 100 + 1) \times 99 + 1$$

$$= 37 \times 99 \times 100 + 100 = (37 \times 99 + 1) \times 100$$

$$\therefore\ \underline{x} = 37 \times 99 + 1 = 3664$$

4. (a). Codewords of C consist of all the linear combinations of $\underline{x}, \underline{y}$

$$\begin{cases} \underline{x} = 0212 \\ \underline{y} = 2011 \end{cases}$$

$0\underline{x}+0\underline{y} = 0000$ $\quad$ $0\underline{x}+1\underline{y} = 2011$ $\quad$ $0\underline{x}+2\underline{y} = 1022$.

$1\underline{x}+0\underline{y} = 0212$ $\quad$ $1\underline{x}+1\underline{y} = 2220$ $\quad$ $1\underline{x}+2\underline{y} = 1201$

$2\underline{x}+0\underline{y} = 0121$ $\quad$ $2\underline{x}+1\underline{y} = 2102$ $\quad$ $2\underline{x}+2\underline{y} = 1110$

(b) Check that if $\underline{c} \in C$, and $\underline{c} \neq \underline{0}$, then $w(\underline{c}) = 3$.

$\Rightarrow d(C) =$ minimum nonzero codeword weight $= 3$.

(c) Sphere-packing bound:

$$|C| \leq \frac{3^4}{1+\binom{4}{1}(3-1)} = \frac{81}{1+8} = 9. \qquad ①$$

And from (a), we know that $|C| = 9$.

So ① holds with equality.

$\therefore$ By definition, C is perfect.

5 (a) E_n is obviously a subset of $V(n,2)$, so it remains to check that E_n is closed under addition and multiplication by constant.

(1) Addition:

Let $\underline{x}, \underline{y} \in E_n$ $\Rightarrow$ $w(\underline{x}), w(\underline{y})$ are both even

$\therefore$ $w(\underline{x}+\underline{y}) = w(\underline{x}) + w(\underline{y}) - 2w(\underline{x} \cap \underline{y})$

$=$ even $+$ even $-$ even $=$ even

$\Rightarrow$ $\underline{x}+\underline{y} \in E_n$ $\Rightarrow$ E_n is closed under addition.

(2) Multiplication. since $q=2$, the only two constants are 0 and 1.

if $\underline{x} \in E_n$, then $0\underline{x} = \underline{0} \in E_n$ since $w(\underline{0}) = 0 =$ even.

$1\underline{x} = \underline{x} \in E_n$.

$\Rightarrow$ E_n is closed under multiplication.

(b). We know that $|V(n-1, 2)| = 2^{n-1}$

because for a length $(n-1)$ vector, at each position, we have two choices.

And. $|E_n| = |V(n-1,2)| = 2^{n-1}$

because for every $\underline{w} \in V(n-1,2)$, there is exactly one $\underline{x} \in E_n$ s.t.

the first $(n-1)$ entries being $\underline{w}$, namely $\begin{cases} \underline{w}0 & \text{if } w(\underline{w}) \text{ is even.} \\ \underline{w}1 & \text{if } w(\underline{w}) \text{ is odd.} \end{cases}$

Or alternatively, we know that $|V(n,2)| = 2^n$,

By symmetry, or by the above argument, the number of even weight in $V(n,2)$ equals the number of odd weight vectors in $V(n,2)$.

$\Rightarrow$. $|E_n| = \frac{1}{2}|V(n,2)| = 2^{n-1}$

For any subspace, we know that the number of vectors $= q^{\text{dimension}} = 2^{n-1}$

$\Rightarrow$. $\mathrm{Dim}(E_n) = n-1$