1 At the end of each period, the wheel will return to its original state, so the period of a pinwheel machine is a multiple of any wheel's size. The minist multiple is the real period. that is $lcm(l_1 \dots l_n)$

So the machine has maximal period only if $l_1 \dots l_n$ are relatively prime.

2. period = lcm (18, 17, 15, 13, 11) = 218790

5-bit number straight up: 01100

5-bit number after 2^{16} steps: 01110

x_0: $2^{16} \bmod 18 = 16$, $6+16 \pmod{18} = 4$ (0)

x_1: $2^{16} \bmod 17 = 1$, $4+1 \pmod{17} = 5$ (1)

x_2: $2^{16} \bmod 15 = 1$, $13+1 \pmod{15} = 14$ (1)

x_3: $2^{16} \bmod 13 = 3$, $1+3 \pmod{13} = 4$ (1)

x_4: $2^{16} \bmod 11 = 9$. $9+9 \pmod{11} = 7$ (0)

3. (1) the expected fraction of the time:

wheel 1: 100%

wheel 3: $\frac{100\%}{16} = 6.25\%$

wheel 5: $\frac{100\%}{16^2} \approx 0.39\%$

wheel 2: $\frac{100\%}{16^3} \approx 0.024\%$

wheel 4: $\frac{100\%}{16^4} \approx 0.0015\%$

each cipher rotor: $1 - \frac{C_{12}^3}{C_{16}^3} = 60.71\%$

(2) when the wheels only includes the control rotors:

$$\frac{15}{16}\times 1+\frac{1}{16}\times\frac{15}{16}\times 2+\frac{1}{16^2}\times\frac{15}{16}\times 3+\frac{1}{16^3}\times\frac{15}{16}\times 4+\frac{1}{16^4}\times 5\approx 1.067$$

when the wheels includes both control and cipher rotors:

$$1\times\frac{C_4^1\times C_4^1}{C_{16}^3}+2\times\frac{C_4^2\times C_2^1\times C_4^1\times C_4^1}{C_{16}^3}+3\times\frac{C_4^3\times C_4^1\times C_4^1\times C_4^1}{C_{16}^3}+1.067\approx 3.5$$

4. (1) $C_4^1+C_4^2+C_4^3=4+6+4=14$

(2) 1 wheel: A: $\frac{C_4^1}{C_{16}^3}=\frac{1}{140}\approx 0.71\%$ (B, C, D is the same)

So the frequency of 1 wheel rotating is $4\times\frac{C_4^1}{C_{16}^3}=\frac{1}{35}\approx 2.86\%$

2 wheels: AB: $\frac{C_2^1\times C_4^1\times C_4^1}{C_{16}^3}=\frac{3}{35}\approx 8.57\%$ (AC, AD, BC, BD, CD is the same)

So the frequency of 2 wheels ~~rotating~~ is $6\times\frac{3}{35}=\frac{18}{35}\approx 51.4\%$

3 wheels: ABC: $\frac{C_4^1\times C_4^1\times C_4^1}{C_{16}^3}=\frac{4}{35}\approx 11.4\%$ (ACD、BCD、ABD is the same)

So the frequency of 3 wheels rotating is $4\times\frac{4}{35}=\frac{16}{35}\approx 45.7\%$

5. $f(x_0,\ldots,x_{n-1})=x_0\oplus g(x_1,\ldots,x_{n-1})$

Proof: Suppose that the shift register is not invertible under this form. then there are 2 different states $S_1=(x_0,x_1,\ldots,x_{n-1})$ and $S_2=(y_0,y_1,\ldots,y_{n-1})$

The next state of both is $z=h(s_1)=h(s_2)$

(set $h(s)$ be the next state of s)

because $h(x_i)=x_{i+1}$, for $i=0,\ldots,n-2$

$x_i=y_i$, $i=1,2,\ldots,n-1$

then $g(x_1,\ldots,x_{n-1})=g(y_1,\ldots,y_{n-1})$

Since $S_1\neq S_2$, $x_0\neq y_0$ (namely $y_0=\bar{x}_0$)

$f(x_0, \ldots, x_{n-1}) \neq f(y_0, \ldots, y_{n-1})$

then $h(s_1) \neq h(s_2)$, contradict