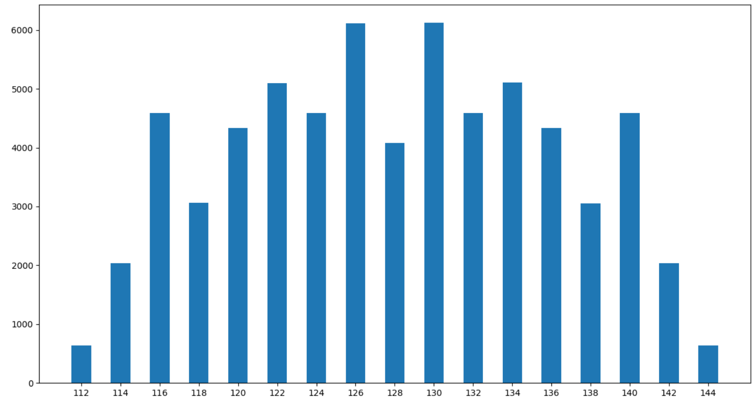
Q1

The counts are non-negative even integers. The counts are even since (assuming that the counts that are being referred to include atleast one input and atleast one output) for every input and output conforming to the count(ie, assume that the accumulated sum of inputs' bits is I and that of outputs' bits is I, then we would've $I \oplus O = 0$) we have the following : - $!I \oplus !O = 0$ - If $I = \oplus i_k$, then $!I = !i_1 \oplus i_k$ and similarly for the outputs - Since I and O both have atleast one input and one output, for every pair of I and O; there exists a pair of $!I$ and $!O$ distinct from the I and O; and hence, the counts would have to be even.

The time complexity of the computation is $O(2^{2^n})$ for all input combinations times $O(2^{2^n})$ for all output combinations times $O(2^{2^n})$ for all inputs to calculate the bias (ignoring -1 for both input mask and output mask) $= O(2^{2^{3n}}) = O((2^{2^n})^3)$ where n is the size of the S-box in bits, here $n = 8$, hence in numerical terms, the time complexity is $O(2^{2^{24}})$.

The **bias table** (the table containing the counts) is included in this folder (table.txt) and the histogram is as follows -


0
1000
2000
3000
4000
5000
6000
112
114
116
118
120
122
124
126
128
130
132
134
136
138
140
142
144