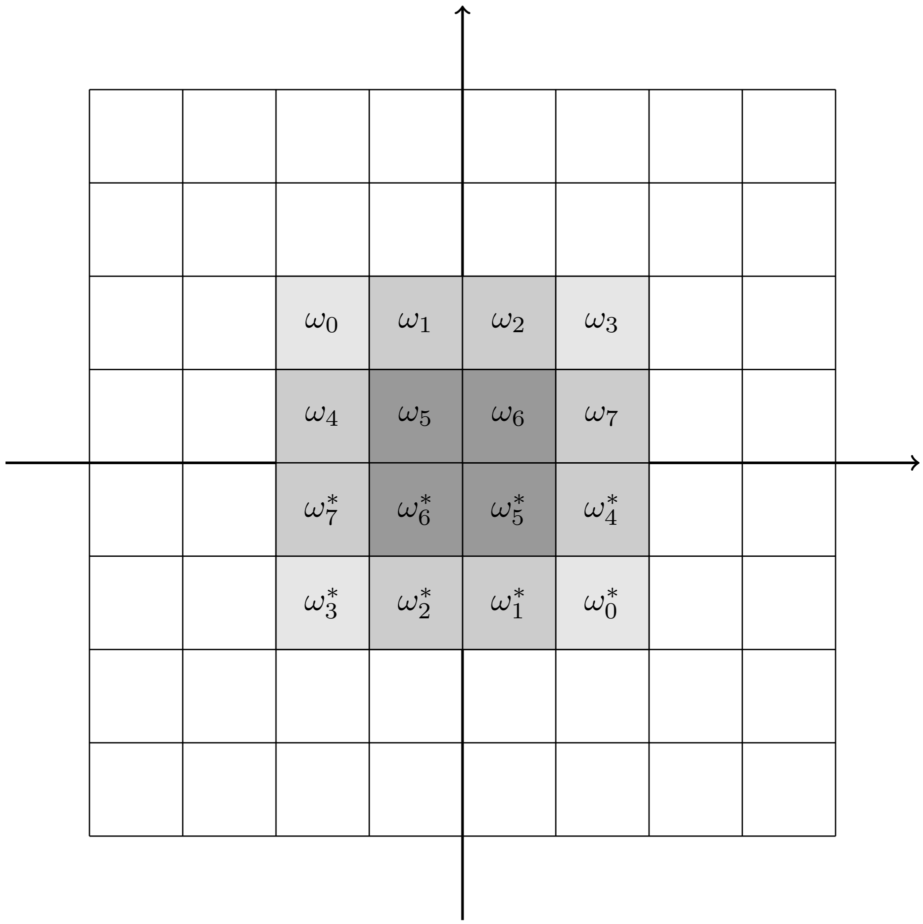


Figure 1: Caption

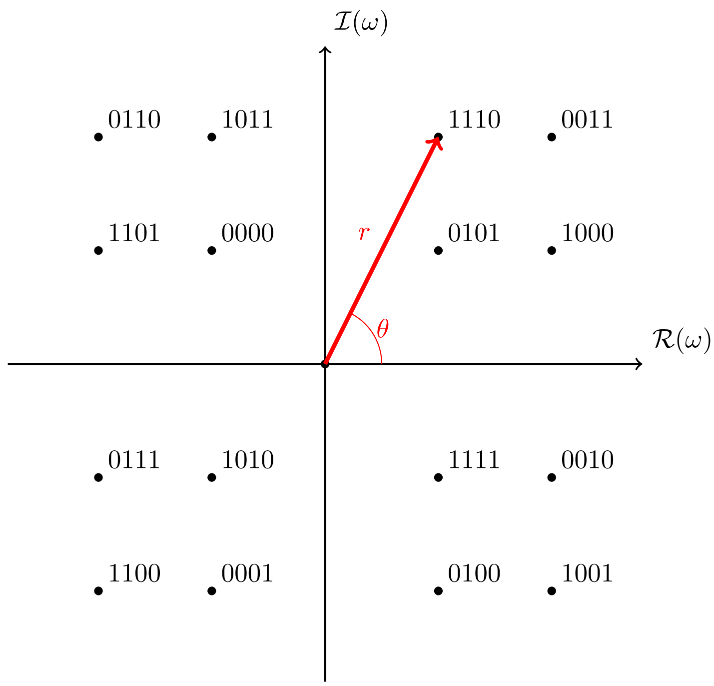
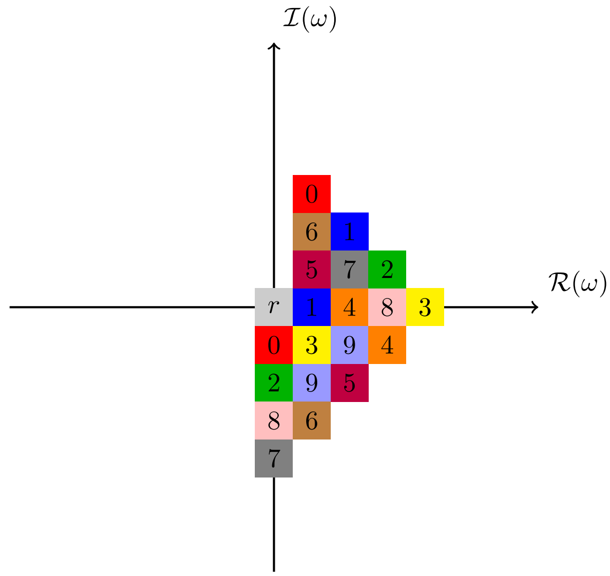


Figure 2: Encoding 4-bit words into frequencies.



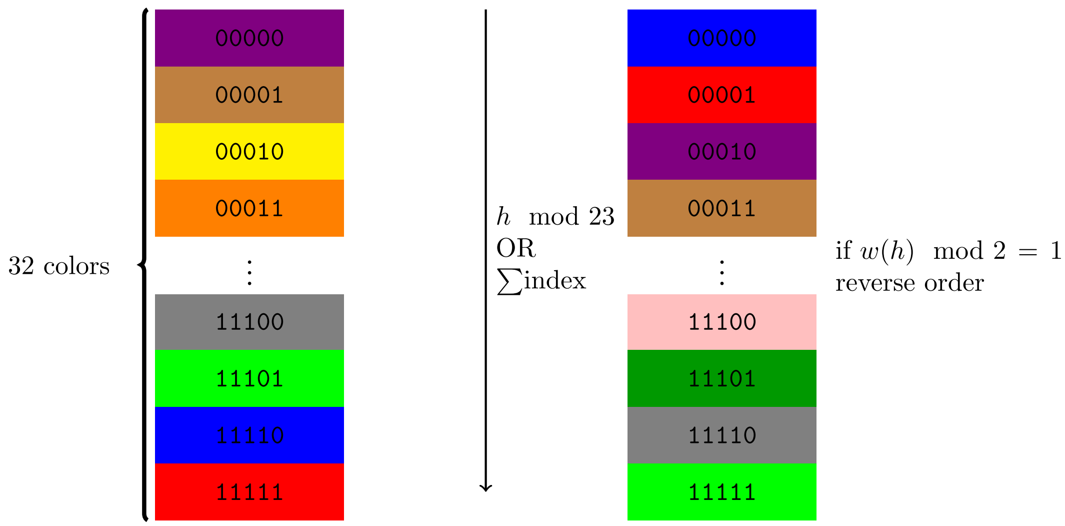
$$\mathcal{B}_m = I(f_m > 0.5),\ m \in \{1, 2, 3\}$$

$$\mathcal{P}(\{\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3\}) \rightarrow \{Color\#1, Color\#2, \ldots, Color\#2^m\}$$

$$\begin{aligned}\{Color\#1, Color\#2, \ldots, Color\#2^m\} = \{& f_1 \leq 0.5 \land f_2 \leq 0.5 \land f_3 \leq 0.5, \\ & f_1 \leq 0.5 \land f_2 \leq 0.5 \land f_3 > 0.5, \\ & \ldots, \\ & f_1 > 0.5 \land f_2 > 0.5 \land f_3 > 0.5\end{aligned}$$

$$h = \underbrace{\underline{1}100}_{f_1} \mid \underbrace{1000}_{f_2} \mid \underbrace{\underline{0}110}_{f_3} \mid \underline{1}110 \mid 0101 \mid 1011 \mid \underline{0}100 \mid 1111 \mid 0110 \mid \underline{0}010 \mid 1001 \mid 0110 \ldots \underline{0}010 \mid 1001 \mid 0101 \mid 1001 \mid 0100$$

$$p_i = \begin{cases} b_{0,i} \oplus b_{1,i} \oplus b_{2,i} \oplus \cdots \oplus b_{9,i} = \bigoplus_{k=0}^{9} b_{k,i} & 0 \leq i < 12 \\ h_{120+i-12} \oplus h_{120+i-8} & 12 \leq i < 16 \end{cases}$$



$$\sum \text{index} = \sum_{k=0}^{128} I(b_k = 1)k \mod 31$$

Proof that $\tilde{x} \neq x \mod 23$, where $\tilde{x}$ is x with 2 bits of the same group changed: Let ℓ and $\ell + 12m$ the indices of the 2 flipped bits, with $0 < m \leq 10$.

Ring of $\mathbb{Z}_p$ is an integral domain.

- Case $b_\ell = 1, b_{\ell+12m} = 0$:

$$\begin{aligned}
& x = \tilde{x} = x - 2^\ell + 2^{\ell+12m} \mod 23 \\
\implies & x = x + 2^\ell \left(2^{12m} - 1\right) \mod 23 \\
\implies & 0 = 2^\ell \left(2^{12m} - 1\right) \mod 23 \\
\implies & 0 = 2^{12m} - 1 \mod 23 \\
\implies & 1 = 2^{12m} \mod 23
\end{aligned}$$

  which has no solution for $1 < m \leq 10$.

- Case $b_\ell = 0, b_{\ell+12m} = 1$:

$$\begin{aligned}
& x = \tilde{x} = x - 2^\ell + 2^{\ell+12m} \mod 23 \\
\implies & x = x + 2^\ell \left(1 - 2^{12m}\right) \mod 23 \\
\implies & 0 = 2^\ell \left(1 - 2^{12m}\right) \mod 23
\end{aligned}$$

  which has no solution for $1 < m \leq 10$, same as the previous case.

- Case $b_\ell = 1, b_{\ell+12m} = 1$:

$$\begin{aligned} x = \tilde{x} &= x + 2^\ell + 2^{\ell+12m} \mod 23 \\ \implies x &= x + 2^\ell \left(1 + 2^{12m}\right) \mod 23 \\ \implies 0 &= 2^\ell \left(1 + 2^{12m}\right) \mod 23 \\ \implies 0 &= 1 + 2^{12m} \mod 23 \\ \implies -1 &= 2^{12m} \mod 23 \end{aligned}$$

  which has no solution for $1 < m \leq 10$.

- Case $b_\ell = 0, b_{\ell+12m} = 0$:

$$\begin{aligned} x = \tilde{x} &= x - 2^\ell - 2^{\ell+12m} \mod 23 \\ \implies x &= x + 2^\ell \left(-1 - 2^{12m}\right) \mod 23 \\ \implies 0 &= 2^\ell \left(-1 - 2^{12m}\right) \mod 23 \end{aligned}$$

  which has no solution for $1 < m \leq 10$, same as the previous case

Attacks if shift is mod 23:

- Adv flips n bits of the same index, keeping same modulo 23 :
  - Effect : the same palette is used. If n is even and $n > 2$, then all colors are exactly the same as intra group parity is the same
  - "Impossible" for odd n as palette is flipped
  - Rare (I guess) for $n = 4$: maximum 8 if the ten bits are e.g. 1101011100
- Adv flips n bits, keeping same modulo 23 :
  - Effect : the same palette is used. The colors corresponding to the n indices are changed
  - "Impossible" for odd n as palette is flipped

$$\begin{aligned} x + 2^k - 2^\ell &= x \mod p \\ 2^k - 2^\ell &= 0 \mod p \\ 2^\ell \left(2^{k-\ell} - 1\right) &= 0 \mod p \\ 2^{k-\ell} &= 1 \mod p \\ k - \ell &= m \cdot |2| \mod p,\ m \in \mathbb{Z} \end{aligned}$$

Problem : 11 is $-1 \mod 12 \implies$ flipping b_i and b_{i+11} might only change 1 color.

Attacks if shift is $\sum index$:

Lots (sum of 4 indices that are for the same function divide 31)