Boolean Algebra

1 Majority function

$$Maj(x, y, z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$$

For each bit index, that result bit according to what bit is the the majority amongst x, y, and z at this index.

2 Choose function

$$Ch(x, y, z) = (x \wedge y) \oplus (\neg x \wedge z)$$

For each bit index, that result bit is according to the bit from y or z, depending on the bit from x.

$$Ch(x, y, z) = \begin{cases} x = 1 & y \\ x = 0 & z \end{cases}$$

3 Parity function

$$Par(x, y, z) = x \oplus y \oplus z$$

Parity is whether it contains an odd or even number of 1-bits.

$$\begin{cases} odd & 1 \\ even & 0 \end{cases}$$

For each bit index, that result bit is according to the parity of x, y, and z at this index.

Bitwise rotation

Also called a circular shift.

$$\begin{aligned}\texttt{bits} &= \text{the number of bits in the field}\\ \texttt{value} &= \text{the field itself}\\ \texttt{n} &= \text{the shift}\end{aligned}$$

4 Rotate left

```
(value << n) | (value >> (bits - n))
```

5 Rotate right

```
(value >> n) | (value << (bits - n))
```