Xorshift

1.初めに

Xorshift乱数生成器(RNG)は, ビットシフトとXOR(排他的論理和)からなる処理で $2^{32}-1$ 個の x , $2^{64}-1$ 個の x, y , $2^{96}-1$ 個の x, y, z などの順序付けられた要素の集合(シーケンス)である. C言語では, 左シフトは, `y^(y<<a)` , 右シフトは, `y^(y>>a)` で表す. Xorshiftの操作は高速かつ秒間 2 億回以上の速度で動作する.

理論

m 個の要素からなるシードセット Z を持ち, Z 上の一対一の関数 $f()$ がある.