Suppose there is a function f(x)

, such that f(x) = f(x+1)

and \int_0^1 f(x) > 0

. We can prove that there exists some value x_0

such that for all x > x_0

, \int_{x_0}^{x} f(x) \ge 0

.

Proof: let F(x) = \int_0^x f(t)dt

. F(1) > F(0)

by assumption. F

has a minimum over [0,1]

, call it x_{min}

. By construction, F(x) \ge F(x_{min})

for x_{min} < x \le 1

, and for x > 1

, F(x) > F(x\ mod\ 1) > F(x_{min})

. Therefore, for all x > x_{min}

, \int_{x_{min}}^{x} f(x) \ge 0

.

Now, here's the relevance to consensus. Suppose that we have a set of validators that is shuffled into an ordered list, and the ordering of the list represents the ordering of the right to create blocks at particular times. The list is repeated over and over again (ie. it's a round robin with an ordering determined by some initial shuffling). Let A(y) - A(x)

be the portion of attackers between x

and y

. Suppose attackers have less than 50% of all validators, so A(1) - A(0) < 0.5

. Define H(x) = x - A(x)

("honest validators"), and F(x) = H(x) - A(x) = x - 2 * A(x)

. F

clearly satisfies the above criterion. F(y) - F(x)

can be interpreted as "the advantage of honest validators within [x,y]

". The above theorem then implies that there is some x_{min}

such that, if you publish a transaction at time x_{min}

(or more generally, x_{min} + k

for k \in Z

), in any time slice (x_{min}, T)

the majority of validators will be honest, which means that the block that immediately includes the transaction will never get overtaken. Hence, an attacker with less than 50% cannot censor a transaction for longer than one cycle.