OGL

Theorem 0.1 (ogl)**.** For any cyclic group G with cardinality s and generator g, $g \neq g^0$, there exists a function $f : G^2 \to G$ such that f can be complexly composed with itself to form any function mapping $G^2 \to G$.

Let op be the function $op(x, y) = x == y?x * g : C$ where C is any element in G. Let $logish$ be the function $logish : G \to Z_{|G|}$ with rule $logish(g^n) = n$. To prove that op satifies ' '0.1 we will prove the following lemmas.

Lemma 0.2 (rot)**.** let rot_n be the function $rot_1(x) = op(x, x)$, $rot_n = rot(rot_{n-1})$ and $rot_0(x) = x$. rot_n will also have the rule $rot_n(x) = x * g^n$.

Corollary 0.2.1. let the functions A_n and B_n have the rule $A_n(x, y) = rot_n(x) = x * g^n$ and $B_n(x, y) = rot_n(y)$. Thus, $A_n(x) = x * g^n$ and $B_n = y * g^n$.

Lemma 0.3 (F-funcs)**.** Let $F_{a,b}$ be a function where $F_{a,b}(x, y) = rot_b(op(A_a(x, y), B_b(x, y)))$. Thus, $F_{a,b}(x, y) = x == y?x * g^{a+b+1} : C * g^b$.

Lemma 0.4 (N-funcs)**.** Let $\overline{a}(x, y) = rot_a(op(A_0(x, y), A_1(x, y)))$. Thus, $\overline{a}(x, y) = C * g^a$.

Lemma 0.5 (isolator)**.** Let $\overline{(a, b, c)}(x, y) = op(F_{logish(c)-logish(C),-logish(C)}(A_a, B_b), \overline{g})$, then $\overline{(a, b, c)}(x, y) = (x == g^a) \wedge (y == g^b)?c : C$

Lemma 0.6 (S)**.** Let $\overline{S_a}(x, y) = F_{-a+logish(C)-1,a-logish(C)}(\overline{(g^0, a, a)}(x, y), \overline{(a, g^0, a)}(x, y))$, then when $a \neq g^0$ $\overline{S_a} = (x == g^a \wedge y == g^0) \vee (x == g^0 \wedge y == g^a)?g^a : C$

Lemma 0.7 (AS)**.** Let $\overline{AS_a}b(x, y) =$