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 $rot_1(x) = op(x, x)$, $rot_n = rot_1(rot_{n-1})$ 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 $\overline{F_{a,b}}$ be a function where $\overline{F_{a,b}}(x, y) = rot_b(op(A_a(x, y), B_a(x, y)))$. Thus, $\overline{F_{a,b}}(x, y) = x == y?x * g^{a+b+1} : C * g^b$.

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

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

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

Lemma 0.7 (AS)**.** Let $\overline{AS_{a,b}}(x, y) = \overline{F_{-b+logish(C)-1,b-logish(C)}}(\overline{S_a}(x, y), \overline{S_{a+1}}(x, y))$

Lemma 0.8 (PCO)**.** let $\overline{PCO_0}(x, y) = \overline{0}(x, y)$, $\overline{PCO_1}(x, y) = \overline{S_1}(x, y)$, $\overline{PCO_2}(x, y) = \overline{F_{logish(C)-2,1-logish(C)}}(\overline{S_2}(x, y), \overline{AS_{1,2}}(x, y))$, and $\overline{PCO_a}(x, y) = \overline{F_{logish(C),-logish(C)}}(h_a, k_a)$

where $h_a(x, y) = (x \in \{g^b \| 1 \leq b \leq a\} \wedge y == g^0) \to g^{logish(x)-1}$, $(y \in \{g^b \| 1 \leq b \leq a\} \wedge x == g^0) \to g^{logish(y)-1}$, $else \to g^0$

and $k_a(x, y) = (x \in \{g^b \| 2 \leq b \leq a\} \wedge y == g^0) \to g^{logish(x)-1}$, $(y \in \{g^b \| 2 \leq b \leq a\} \wedge x == g^0) \to g^{logish(y)-1}$, $else \to g^1$

then $\overline{PCO_a}(x, y) = (x \in \{g^b \| 0 \leq b \leq a\} \wedge y == g^0) \to x$, $(y \in \{g^b \| 2 \leq b \leq a\} \wedge x == g^0) \to y$, $else \to g^0$

Lemma 0.9. Let $P(x, y)$ be an arbituary function in G where $P(a, b) = g^{p_{a,b}}$ and for every $a, b \in G$, $p_{a,b} \leq c$ then

$$\begin{aligned} P(x, y) = {} & \overline{(0, 0, p_{0,0})}(x, y)\text{“}\overline{PCO_c}\text{''}\overline{(0, 1, p_{0,1})}(x, y)\text{“}\overline{PCO_c}\text{''} \ldots \text{“}\overline{PCO_c}\text{''}\overline{(0, s, p_{0,s})}(x, y) \\ & \text{“}\overline{PCO_c}\text{''}\overline{(1, 0, p_{1,0})}(x, y)\text{“}\overline{PCO_c}\text{''}\overline{(1, 1, p_{1,1})}(x, y) \ldots \text{“}\overline{PCO_c}\text{''}\overline{(1, s, p_{1,s})}(x, y) \\ & \text{“}\overline{PCO_c}\text{''} \ldots \text{“}\overline{PCO_c}\text{''}\overline{(s, s, p_{s,s})}(x, y) \end{aligned} \tag{1}$$

where $x\text{“}f\text{''}y = f(x, y)$

rot. We will prove that $rot_n(x) = x*g^n$ by mathematical induction. Let $P(n) = rot_n(x)$. First, we will show that $P(1) = x*g$. Since $P(1) = rot_1(x)$, $rot_1(x) = op(x, x) = x == x?x * g : C$ and $x == x$ is true, $P(1) = x * g$. Next, we prove the inductive step. Let k be an arbitrary natural number and assume that $P(k)$ is true meaning

(1) $P(k) = rot_k(x) = (rot_1 \circ rot_1 \circ \ldots \text{k-times} \cdots \circ rot_1)(x) = x * g^k$

We will now prove $P(k + 1)$ is true, that is

(2) $P(k + 1) = (rot_1 \circ rot_1 \circ \ldots \text{k+1-times} \cdots \circ rot_1)(x) = x * g^{k+1}$

By replacing (1) into (2) we obtain $P(k + 1) = rot_1(P(k)) = rot(x * g^k) = (x * g^k) * g = x * g^{k+1}$

This proves the inductive step and by the principle of mathematical induction, the lemma is proved. □

F-funcs. We will prove that $\overline{F_{a,b}}(x, y) = x == y?x * g^{a+b+1} : C * g^b$. Let us consider 2 cases, when $x = y$ and $x \neq y$. When $x = y$, we show that $\overline{F_{a,b}}(x, x) = x * g^{a+b+1}$

$$\begin{aligned} \overline{F_{a,b}}(x, x) &= rot_b(op(A_a(x, x), B_a(x, x))) \\ &= rot_b(op(x * g^a, x * g^a)) \\ &= rot_b(x * g^a * g) \\ &= x * g^a * g * g^b \\ &= x * g^{a+1+b} \end{aligned} \tag{2}$$

Since $x * g^{a+1+b} = \overline{F_{a,b}}(x,x) = x * g^{a+b+1}$, this case is shown. In the case that $x \neq y$, we show that $\overline{F_{a,b}}(x,y) = C * g^b$

$$\begin{aligned} \overline{F_{a,b}}(x,y) &= rot_b(op(A_a(x,y), B_a(x,y))) \\ &= rot_b(op(x * g^a, y * g^a)) \\ &= rot_b(C) \\ &= C * g^b \end{aligned} \tag{3}$$

This shows that $\overline{F_{a,b}}(x,y) = C * g^b$ when $x \neq y$. Since both cases are shown, the lemma follows. □

N-funcs. We will show that $\overline{a}(x,y) = g^a$. From the definition $\overline{a}(x,y) = rot_{a-logish(C)}(op(A_0(x,y), A_1(x,y)))$ or

$$\begin{aligned} \overline{a}(x,y) &= rot_{a-logish(C)}(op(A_0(x,y), A_1(x,y))) \\ &= rot_{a-logish(C)}(op(x, x * g)) \\ &= rot_{a-logish(C)}(C) \\ &= C * g^{a-logish(C)-1} \\ &= g^{logish(C)} * g^{a-logish(C)} \\ &= g^{logish(C)+a-logish(C)} \\ &= g^a \end{aligned} \tag{4}$$

Thus, $\overline{a}(x,y) = g^a$. □

isolator. We will show that $\overline{(a,b,c)}(x,y) = (x == g^a) \wedge (y == g^b)?c : C$. Let us consider the two cases where $x = g^a \wedge y = g^b$ and where $x \neq g^a \vee y \neq g^b$. From the definition, $\overline{(a,b,c)}(x,y) = op(\overline{F_{logish(c)-logish(C),-logish(C)}}(A_a(x,y), B_b(x,y)), \overline{g}(x,y))$, so when $x = g^a \wedge y = g^b$

$$\begin{aligned} \overline{(a,b,c)}(g^a, g^b) &= op(\overline{F_{logish(c)-logish(C),-logish(C)}}(A_a(g^a, g^b), B_b(g^a, g^b)), \overline{g}(g^a, g^b)) \\ &= op(\overline{F_{logish(c)-logish(C),-logish(C)}}(g^{2a}, g^{2b}), g) \\ &= op(\overline{F_{logish(c)-logish(C),-logish(C)}}(g^a, g^b), g) \\ &= op(\overline{F_{logish(c)-logish(C),-logish(C)}}(g^a, g^b), g) \end{aligned} \tag{5}$$

□