Solution of UyHiP 2017 May

Hanlin Ren

May 3, 2017

1 Answer

Let $P(n)$ be the statement : "it's possible to find an abelian group $(G,+)$ of size n and bijections $A,B,C : G \to G$ such that $\forall x \in G,\ A(x)+B(x)=C(x)$". Then $n \not\equiv 2 \pmod 4 \implies P(n)$.

On the other hand, when $n \equiv 2 \pmod 4$, we can't find group G and bijections A,B,C that satisfies the condition, even if G can be non-abelian. Therefore the answer for part 1 and part 2 are both $n \not\equiv 2 \pmod 4$.

2 Proof for $n \not\equiv 2 \pmod 4$ case

Lemma 1. $n \equiv 1 \pmod 2 \implies P(n)$.

Proof. Let $G = (\mathbb{Z}/n\mathbb{Z},+)$, since n is odd, $x \mapsto (x+x) \bmod n$ is a bijection. We let $A(x)=B(x)=x$, $C(x)=(x+x) \bmod n$. □

Lemma 2. $P(4)$.

Proof. Let G be the set of all binary strings of length 2, $+$ is the xor operation, and A,B,C are defined as follows :

$x=$	00	01	10	11
$A(x)=$	00	01	10	11
$B(x)=$	00	11	01	10
$C(x)=$	00	10	11	01

It's easy to check A,B,C are all bijections and $\forall x \in G,\ A(x)+B(x)=C(x)$. □

Lemma 3. $P(8)$.

Proof. Let G be the set of all binary strings of length 3, $+$ is the xor operation, and A,B,C are defined as follows :

$x=$	000	001	010	011	100	101	110	111
$A(x)=$	000	001	010	011	100	101	110	111
$B(x)=$	000	111	101	010	110	001	011	100
$C(x)=$	000	110	111	001	010	100	101	011

It's easy to check A,B,C are all bijections and $\forall x \in G,\ A(x)+B(x)=C(x)$. □

Lemma 4. $\forall n_1,n_2 \in \mathbb{Z},\ P(n_1) \wedge P(n_2) \implies P(n_1n_2)$.

Proof. Suppose $P(n_1) \wedge P(n_2)$. Then there exists abelian groups $(G_1,+_1),(G_2,+_2)$ and bijections $A_1,B_1,C_1 : G_1 \to G_1$ and $A_2,B_2,C_2 : G_2 \to G_2$ that $|G_1|=n_1, |G_2|=n_2$, $\forall x \in G_1, A_1(x) +_1 B_1(x) = C_1(x)$, and $\forall x \in G_2, A_2(x) +_2 B_2(x) = C_2(x)$.

Let G be the direct sum $G_1 \oplus G_2$, then G is abelian. Let $A(x,y)=(A_1(x),A_2(y))$, $B(x,y)=(B_1(x),B_2(y))$, $C(x,y)=(C_1(x),C_2(y))$. It's easy to check that A,B,C are bijections from G to itself, and $\forall x \in G_1, y \in G_2$, $A(x,y)+B(x,y)=(A_1(x)+_1B_1(x),A_2(y)+_2B_2(y))=(C_1(x),C_2(y))=C(x,y)$. Since $|G|=n_1n_2$, $P(n_1n_2)$ is true. □

Theorem 5. $n \not\equiv 2 \pmod 4 \implies P(n)$.

Proof. From lemma 1, we know that $n \not\equiv 1 \pmod 2 \implies P(n)$. Now we concentrate on the case that $n \equiv 0 \pmod 4$. Let $n = 2^s(2t+1)$, where $s, t \in \mathbb{Z}$. Since $n \equiv 0 \pmod 4$, $s \geq 2$. If $s \equiv 0 \pmod 2$, we write $n = 4^{s/2}(2t+1)$; otherwise $s \geq 3$ and we can write $n = 4^{(s-3)/2} \cdot 8 \cdot (2t+1)$. Since $P(4), P(8), P(2t+1)$, we know that $P(n)$ is true. □

3 Proof for $n \equiv 2 \pmod 4$ case

Now we consider $n \equiv 2 \pmod 4$. We show that even if the restriction that G is abelian is removed, no group G and bijections A, B, C satisfies $\forall x \in G, A(x)B(x) = C(x)$.

Note : in the non-abelian case, operator $*$ is omitted.

Lemma 6. *Suppose G is a group, and $|G| = n = 4k+2$ for some $k \in \mathbb{Z}$. Then G has a subgroup of size $2k+1$.*

Proof. By Cayley's theorem, G is isomorphic to some subgroup $G' \leq S_n$. So we only need to prove the theorem for G'. Moreover, suppose the group isomorphic function is f, then $\forall g, h \in G$, $f(g)$, which is some element in G', maps h to gh.

Since $2 \mid n$, there is an element $u \in G$ that $o(u) = 2$, where $o(x)$ is the order of x. There are $\frac{n}{o(u)}$ cycles in the permutation $f(u)$, each of length 2, so $f(u)$ is an odd permutation. Since there is an odd permutation in G', there are $\frac{|G'|}{2}$ odd permutations in G', and the even permutations in G' forms a subgroup of size $2k+1$. □

Theorem 7. *When $n \equiv 2 \pmod 4$, it's impossible to find a group G of size n and three bijections $A, B, C : G \to G$ such that $\forall x \in G$, $A(x)B(x) = C(x)$.*

Proof. Suppose there exists G, A, B, C as the theorem states.

Consider the subgroup H of G which has size $\frac{n}{2}$. For an element x, we define its characteristic function $\chi(x) = \begin{cases} 0 & x \in H \\ 1 & x \notin H \end{cases}$. By the argument above, there exists some element $u \in G$ that $o(u) = 2$ and $u \notin H$. Therefore $G = H \cup uH = H \cup Hu$.

$\forall x, y \in G$:

- If $x, y \in H$, then obviously $xy \in H$.
- If $x \in H, y \notin H$, then $\exists v \in H$, $y = vu$. Therefore $xy = xvu \in Hu$, so $xy \notin H$.
- If $x \notin H, y \in H$, then $\exists v \in H$, $x = uv$. Therefore $xy = uvy \in uH$, so $xy \notin H$.
- If $x, y \notin H$, then $\exists v, w \in H$, $x = vu, y = uw$. Therefore $xy = vu^2w = vw \in H$.

So we proved that $\forall x, y \in G$, $\chi(x) + \chi(y) \equiv \chi(xy) \pmod 2$.

Let's consider $S = \sum_{x \in G} \chi(A(x)) + \chi(B(x)) + \chi(C(x))$. Since $A(x)B(x) = C(x)$, $\chi(A(x)) + \chi(B(x)) + \chi(C(x)) \equiv 0 \pmod 2$, so S is an even number. However $S = 3\sum_{x \in G} \chi(x) = 3(|G| - |H|) = \frac{3n}{2}$ is odd. We obtained a contradiction, thus no G, A, B, C satisfying the conditions exist. □