─────────────── MODULE *Integrity* ───────────────

EXTENDS *Naturals, FiniteSets, Sequences, Commons*

CONSTANT *NPROCESSES, NGROUPS, NMESSAGES, CONFLICTR(_, _)*

This algorithm works in an environment with crash-stop failures, but we do not model processes failing. The set of all processes contains all correct ones.

LOCAL *Processes* $\triangleq$ $1 \, .. \, NPROCESSES$
LOCAL *Groups* $\triangleq$ $1 \, .. \, NGROUPS$
LOCAL *ProcessesInGroup* $\triangleq$ $[g \in Groups \mapsto Processes]$

This property verifies that we only deliver sent messages. To assert this, we create *NMESSAGES*+ 1 and do not include the additional one in the algorithm execution, then check that the delivered ones are only the sent ones.

LOCAL *AcceptableMessageIds* $\triangleq$ $\{id : id \in 1 \, .. \, NMESSAGES\}$
LOCAL *AllMessages* $\triangleq$ *CreateMessages*($NMESSAGES + 1$, *Groups, Processes*)
LOCAL *SentMessage* $\triangleq$ $\{m \in AllMessages : m.id \in AcceptableMessageIds\}$

LOCAL *MessagesCombinations* $\triangleq$ *CreatePossibleMessages*(*AllMessages*)
LOCAL *CombinationsToSend* $\triangleq$ $[i \in$ DOMAIN *MessagesCombinations* $\mapsto$
    SelectSeq(*MessagesCombinations*$[i]$, LAMBDA $m : m \in SentMessage$)]

VARIABLES *K, PreviousMsgs, Delivered, Votes, MemoryBuffer,*
    QuasiReliableChannel, AtomicBroadcastBuffer

Initialize the instance for the Generic Multicast 2. The *INITIAL_MESSAGES* is a sequence, partially ordered. The sequence elements are sets of messages, messages that commute can share a set.

Algorithm $\triangleq$ INSTANCE *GenericMulticast2* WITH
    INITIAL_MESSAGES $\leftarrow$ $[g \in Groups \mapsto$
        PartiallyOrdered(
            CombinationsToSend$[(g\%NMESSAGES) + 1]$, *CONFLICTR*)]

Spec $\triangleq$ *Algorithm*!*SpecFair* Weak fairness is necessary.

For every message, all the correct processes in the destination deliver it only once, and a process previously sent it.

LOCAL *DeliveredOnlyOnce*(g, p, m) $\triangleq$
    Cardinality(*Algorithm*!*FilterDeliveredMessages*(g, p, m)) $= 1$
Integrity $\triangleq$
    $\Diamond\Box\forall \, m \in AllMessages :$
        $\forall \, g \, \in m.d :$
            $\forall \, p \in ProcessesInGroup[g] :$
                $(p \in Processes \wedge DeliveredOnlyOnce(g, p, m)) \equiv m \in SentMessage$