

Practica 7

Ej 1: Función maxMinMemory programada en Yul para memoria con la función en el bloque assembly fmaxmin:

```
function maxMinMemory(uint[] memory arr) public pure returns (uint maxmin){  
    assembly {  
  
        function fmaxmin(array_pointer) -> maxVal, minVal {  
  
            let len := mload(array_pointer) // cargamos de memoria la longitud del array  
            let data := add(array_pointer, 0x20) // avanzamos a la posicion de memoria del primer elemento  
            maxVal := mload(data)  
            minVal := mload(data)  
            let i := 1  
  
            for {} lt(i, len) { i := add(i, 1) } {  
                let elem := mload(add(data, mul(i, 0x20))) // cargamos el siguiente elemento  
                if gt(elem, maxVal) { // si es mayor el elemento q el maximo -> es el maximo  
                    maxVal := elem  
                }  
                if lt(elem, minVal) { // si es menor el elemento que el minimo -> es el minimo  
                    minVal := elem  
                }  
            }  
        }  
  
        let maxVal, minVal := fmaxmin(arr)  
        maxmin := sub(maxVal, minVal)  
    }  
}
```

```
CALL [call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: lab7.maxMinMemory(uint256[]) data: 0x8fb...00005  
  
from 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4  
  
to lab7.maxMinMemory(uint256[]) 0x7EF2e0048f5bAeDe046f68F797943daF4ED8CB47  
  
execution cost 1286 gas (Cost only applies when called by a contract)  
  
input 0x8fb...00005  
  
decoded input {  
    "uint256[] arr": [  
        "1",  
        "2",  
        "3",  
        "4",  
        "5"  
    ]  
}  
  
decoded output {  
    "0": "uint256: maxmin 4"  
}  
  
logs []
```

Ej 2: Dado el contrato lab6ex6 programamos la función maxMinStorage que realice el mismo cálculo que el apartado anterior para un array arr en storage. El contrato tiene la variable uint[] arr;

```
function maxMinStorage() public view returns (uint maxmin) {
    uint256 s;

    assembly{
        s := arr.slot
    }

    bytes32 loc = keccak256(abi.encode(s));

    assembly {
        //no se si es asi, muy parecido al anterior
        function fmaxmin(slot, n) -> maxVal, minVal {
            let len := sload(n)
            maxVal := sload(slot)
            minVal := sload(slot)

            for {let i := 1} lt(i, len) { i := add(i, 1) } {
                let elem := sload(add(slot, i))
                if gt(elem, maxVal) { // si es mayor el elemento q el maximo -> es el maximo
                    maxVal := elem
                }
                if lt(elem, minVal) { // si es menor el elemento que el minimo -> es el minimo
                    minVal := elem
                }
            }
        }

        let maxVal, minVal := fmaxmin(loc, arr.slot)
        maxmin := sub(maxVal, minVal)
    }
}
```

```

[vm] from: 0x5B3...eddC4 to: lab6ex6.generate(uint256) 0xd91...39138 value: 0 wei data: 0x4a7...00064 logs: 0 hash: 0xe08...fc92a
status      0x1 Transaction mined and execution succeed
transaction hash  0xe0808284bd58b7cb33baa367fb78e685dac2432d9897c3cadcle119452bfc92a
block hash      0x3dc19da727c1354894acall131408c0523def9ba69dbcdde5c044f2fd8cd6c29
block number    2
from           0x5B380a6a701c568545dCfcB03FcB875f56beddC4
to            lab6ex6.generate(uint256) 0xd9145CCE520386f254917e481eB44e9943F39138
gas            2644719 gas
transaction cost 2299755 gas
execution cost  2278551 gas
input          0x4a7...00064
decoded input   {
    "uint256 n": "100"
}
decoded output  {}
logs           []

```

```

CALL [call] from: 0x5B380a6a701c568545dCfcB03FcB875f56beddC4 to: lab6ex6.maxMinStorage() data: 0xb99...9fafd
from           0x5B380a6a701c568545dCfcB03FcB875f56beddC4
to            lab6ex6.maxMinStorage() 0xd9145CCE520386f254917e481eB44e9943F39138
execution cost 224027 gas (Cost only applies when called by a contract)
input         0xb99...9fafd
decoded input  {}
decoded output {
    "0": "uint256: maxmin 240"
}
logs          []

```

Ej 3: Implementación simple de `maxMinStorage()` escrita en Solidity, y creamos un array de 100 elementos para el contrato `lab6ex6` y para este `lab7Simple` para comparar los consumos de gas.

```
function maxMinStorage() public view returns (uint maxmin) {  
    uint max = arr[0];  
    uint min = arr[0];  
    uint elem;  
  
    for(uint i = 1; i < arr.length; i++){  
        elem = arr[i];  
  
        if(elem > max) max = elem;  
        if(elem < min) min = elem;  
    }  
  
    maxmin = max - min;  
}
```

generamos array de 100 elems para el contrato `lab7Simple`

```
[vm] from: 0x5B3...eddC4 to: lab7Simple.generate(uint256) 0xdda...5482d value: 0 wei data: 0x4a7...00064 logs: 0 hash: 0x7c0...58da6  
status 0x1 Transaction mined and execution succeed  
transaction hash 0x7c0584e9747134dc97903943529d8e54203396b8516e90b18cad59f768058da6  
block hash 0x6973ee67327e85bda2f8867a07cd104ee0aeea0bb20e2a01fc2ed1ba1dd4eeef3  
block number 14  
from 0x5B380a6a701c568545dCfcB03FcB875f56beddC4  
to lab7Simple.generate(uint256) 0xddaAd340b0f1Ef65169Ae5E41A8b10776a75482d  
gas 2644719 gas  
transaction cost 229755 gas  
execution cost 2278551 gas  
input 0x4a7...00064  
decoded input {  
    "uint256 n": "100"  
}  
decoded output {}  
logs []
```

Ejecutamos la función `maxMinStorage`:

```
[call] from: 0x5B380a6a701c568545dCfcB03FcB875f56beddC4 to: lab7Simple.maxMinStorage() data: 0xb99...9fafd  
from 0x5B380a6a701c568545dCfcB03FcB875f56beddC4  
to lab7Simple.maxMinStorage() 0xddaAd340b0f1Ef65169Ae5E41A8b10776a75482d  
execution cost 252924 gas (Cost only applies when called by a contract)  
input 0xb99...9fafd  
decoded input {}  
decoded output {  
    "0": "uint256: maxmin 240"  
}  
logs []
```

gas de maxMinStorage para array de 100 elementos en contrato lab6ex6: 224017 gas

gas de maxMinStorage para array de 100 elementos en contrato lab7Simple: 252924 gas

Como podemos apreciar existe una diferencia de gas consumido al hacerlo mediante Yul respecto a hacerlo mediante Solidity simple, esto se debe a que Yul permite escribir en lenguaje a más bajo nivel, estando más cerca del nivel de la máquina virtual Ethereum y esto permite tener un menor consumo de gas respecto a la implementación simple en Solidity.