```
> B2:=array(0..15,[[0,0,0,0],[0,0,0,1],[0,0,1,0],[0,0,1,1],[0,1,0,0],
  [0,1,0,1],[0,1,1,0],[0,1,1,1],[1,0,0,0],[1,0,0,1],[1,0,1,0],[1,0,1,
  1],[1,1,0,0],[1,1,0,1],[1,1,1,0],[1,1,1,1]]):
> x:=[0,0,1,0,0,1,1,0,1,0,1,1,0,1,1,1]:
> PiS:=table():
> PiS[B2[0]]:=B2[14];PiS[B2[1]]:=B2[4];PiS[B2[2]]:=B2[13];PiS[B2[3]]
  :=B2[1];PiS[B2[4]]:=B2[2];PiS[B2[5]]:=B2[15];PiS[B2[6]]:=B2[11];PiS
  [B2[7]]:=B2[8];PiS[B2[8]]:=B2[3];PiS[B2[9]]:=B2[10];PiS[B2[10]]:=B2
  [6];PiS[B2[11]]:=B2[12];PiS[B2[12]]:=B2[5];PiS[B2[13]]:=B2[9];PiS
  [B2[14]]:=B2[0];PiS[B2[15]]:=B2[7];
```

$$PiS_{[0,0,0,0]} := [1,1,1,0]$$
$$PiS_{[0,0,0,1]} := [0,1,0,0]$$
$$PiS_{[0,0,1,0]} := [1,1,0,1]$$
$$PiS_{[0,0,1,1]} := [0,0,0,1]$$
$$PiS_{[0,1,0,0]} := [0,0,1,0]$$
$$PiS_{[0,1,0,1]} := [1,1,1,1]$$
$$PiS_{[0,1,1,0]} := [1,0,1,1]$$
$$PiS_{[0,1,1,1]} := [1,0,0,0]$$
$$PiS_{[1,0,0,0]} := [0,0,1,1]$$
$$PiS_{[1,0,0,1]} := [1,0,1,0]$$
$$PiS_{[1,0,1,0]} := [0,1,1,0]$$
$$PiS_{[1,0,1,1]} := [1,1,0,0]$$
$$PiS_{[1,1,0,0]} := [0,1,0,1]$$
$$PiS_{[1,1,0,1]} := [1,0,0,1]$$
$$PiS_{[1,1,1,0]} := [0,0,0,0]$$
$$PiS_{[1,1,1,1]} := [0,1,1,1] \quad (1)$$

```
> PiP:=[1,5,9,13,2,6,10,14,3,7,11,15,4,8,12,16];
```

$$PiP := [1,5,9,13,2,6,10,14,3,7,11,15,4,8,12,16] \quad (2)$$

```
> K:=[[0,0,1,1,1,0,1,0,1,0,0,1,0,1,0,0],[1,0,1,0,1,0,0,1,0,1,0,0,1,1,
  0,1],[1,0,0,1,0,1,0,0,1,1,0,1,0,1,1,0],[0,1,0,0,1,1,0,1,0,1,1,0,0,
  0,1,1],[1,1,0,1,0,1,1,0,0,0,1,1,1,1,1,1]]:
> SPN := proc(x,PiS,PiP,K) local w,y,v,u,temp::array, Nr,l,m,i,j,
  r::integer;
      w[0]:=x;
      (Nr,l,m):=(4,4,4);
      for r from 1 to (Nr-1) do
          print(r);
          print("w",r-1,w[r-1]);
          print("K",r,K[r]);
          u[r]:=w[r-1]+K[r] mod 2;
          print("u",r,u[r]);
          v[r]:=[];
          for i from 1 to m do
               temp:=PiS[u[r][((i-1)*l+1)..(i*l)]];
```

```
            v[r]:=[op(v[r]),op(temp)];
        end do;
        print("v",r,v[r]);
        w[r]:=[];
        for j from 1 to l*m do
            w[r]:=[op(w[r]),v[r][PiP[j]]];
        end do;
    end do;
    u[Nr]:=w[Nr-1]+K[Nr] mod 2;
    print(Nr);
    print("w",r-1,w[r-1]);
    print("K",r,K[r]);
    print("u",Nr,u[Nr]);
    v[Nr]:=[];
    for i from 1 to m do
        temp:=PiS[u[Nr][((i-1)*l+1)..(i*l)]];
        v[Nr]:=[op(v[Nr]),op(temp)];
     end do;
    print("v",Nr,v[Nr]);
    y:= v[Nr] + K[Nr+1] mod 2:
    print();
    print("K",Nr+1,K[Nr+1]);
    print("y=",y);
end proc:
> SPN(x,PiS,PiP,K);
                                    1
                "w", 0, [0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1]
                "K", 1, [0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0]
                "u", 1, [0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1]
                "v", 1, [0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1]
                                    2
                "w", 1, [0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1]
                "K", 2, [1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1]
                "u", 2, [1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0]
                "v", 2, [0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0]
                                    3
                "w", 2, [0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0]
                "K", 3, [1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0]
                "u", 3, [1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0]
                "v", 3, [1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0]
                                    4
                "w", 3, [1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0]
                "K", 4, [0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1]
                "u", 4, [1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1]
                "v", 4, [0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1]

                "K", 5, [1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1]
```

```
> "y=", [1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0]                    (3)
```