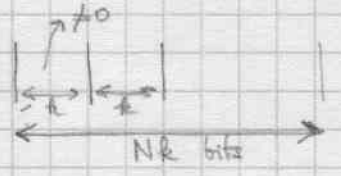
① XRO1: pose en libre $[A2^1] = INT\left(\sqrt[k]{V1[A0]^q}\right)$ conserve A0/D3

$D3^e = k$

$D4^k = \begin{cases} 0 & \text{exact} \\ \neq 1 & \text{approché} \end{cases}$

KL20 : MOVEM.L D3/A0 -(SP)

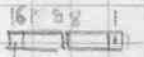
⊗ CMP #2,D3
BNE KL26
BSR SQRT1
MOVEM.L (SP)+,D3/A0
RTS

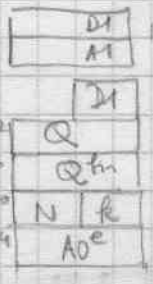
$[A0]^e =$ 

XRO1 : MOVE (A0),D0
CMP #$4000,D0
BEQ KL18
BCLR #15,D0
CMP #$4001,D0
BNE KL20
KL18: MOVE.L A6,A2
MOVE D0,(A6)+
CLR D4
RTS

1000

⊗ KL26 : BSR XBNB

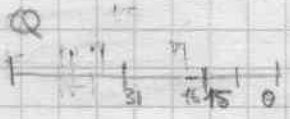




DIVU D3,D1 D1.W = N-1
MOVE D1,(SP)
LEA TCONST2,A0 BSR XXP2N
BSR XEXPD2 $[Q = 2^{N-1}$
MOVE (SP),D1
MOVE.L A2/A6,-(SP)

boucle $i = N-1$ à 0

KL28 : MOVEM.L (SP),A0/A1 Q^m localise le bit i de Q



MOVE D1,-(SP)
KL30 : SUBQ #1,A1
SUBQ #8,D1
BPL KL30
ADDQ #8,D1
BSET D1,(A1) {MOVEM.L D1/A1,-(SP)
MOVE.L 20(SP),D1 $k = D1$
BSR XEXPD2 Q^k
MOVE.L A2,A1 Q^k
MOVE.L 22(SP),A0 $[A0^e]$
MOVE.L A2,A6
BSR XCMP1 cmp $Q^k, [A0]^e$
MOVEM.L (SP)+,D1/A1
X BEQ KL34 → Q = racine
BCC KL32 → $[A0]^e > Q^k$
BCLR D1,(A1)

$Q = Q + 2^i$ (ou 2^{N-1} si $i = N-1$)

(1)

```
KL32 : MOVE   (SP)+, D1
       DBRA   D1, KL28
Q = racine approchée
       MOVEQ  #1, D4
KL33 : MOVEM.L (SP)+, A2/A3
       MOVEM.L (SP)+, D3/A0

       RTS

KL34 : CLR    D4
       ADDQ   #2, SP
       BRA    KL33
```

Q = racine exacte