(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 605 431**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **86 14378**

(51) Int Cl⁴ : G 06 K 19/02.

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 16 octobre 1986.

(30) Priorité :

(43) Date de la mise à disposition du public de la demande : BOPI « Brevets » n° 16 du 22 avril 1988.

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : *ETAT FRANCAIS, représenté par le ministre des PTT, Centre national d'études des télécommunications et Etablissement public de diffusion dit : TELEDIFFUSION DE FRANCE.* — FR.

(72) Inventeur(s) : Louis Guillou.

(73) Titulaire(s) :

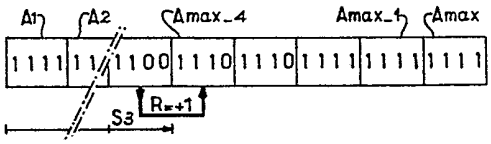
(74) Mandataire(s) : Brevatome.

(54) Procédé de paiement électronique utilisant une carte à mémoire.

(57) Procédé de paiement électronique utilisant une carte à mémoire.

Les cellules de mémorisation sont groupées en éléments groupant au moins deux cellules, chaque élément étant repérable par une adresse et ayant une parité. Le solde de la carte est le nombre d'éléments non nuls pairs d'adresse inférieure à l'adresse de l'élément impair qui a la plus faible adresse et qui est appelée « borne ». Pour débiter la carte et réduire ce solde, on déplace la borne vers une adresse plus basse en créant un nouvel élément impair d'adresse plus faible que la borne à déplacer. Pour créditer la carte et augmenter ce solde, on déplace la borne vers une adresse plus haute, en redonnant aux éventuels éléments impairs d'adresse supérieure à la borne à déplacer un caractère pair et en créant un nouvel élément impair d'adresse plus haute que la borne à déplacer.

Application au paiement électronique.



FR 2 605 431 - A1

Vente des fascicules à l'IMPRIMERIE NATIONALE, 27, rue de la Convention — 75732 PARIS CEDEX 15

PROCEDE DE PAIEMENT ELECTRONIQUE UTILISANT UNE CARTE A MEMOIRE

DESCRIPTION

La présente invention a pour objet un procédé de paiement électronique utilisant une carte à mémoire.

On sait qu'il existe aujourd'hui des moyens électroniques pour effectuer certaines transactions, comme par exemple le paiement de marchandises, l'acquittement de communications téléphoniques ou de services divers. Ce moyen est en plein développement car il offre des avantages considérables de commodité, de rapidité et de sécurité. On a pu parler à ce propos de "monnaie électronique".

Ces moyens utilisent une carte à mémoire qui est un support plastique dans lequel est implanté un composant électronique contenant un microprocesseur. Celui-ci contient une mémoire de données de plusieurs centaines de bits réalisée en technologie "EPROM". Il s'agit là d'une mémoire à lecture seulement, programmable électriquement (Electrically Programmable Read Only Memory).

Le traitement électronique effectué dans une telle carte consiste à faire correspondre à chaque élément binaire (ou bit) d'une zone de la mémoire, une unité de paiement dite "jeton". Un terminal point de vente, muni d'un lecteur de carte, exécute une transaction par "grillage" d'un certain nombre de bits dans la mémoire. Le "grillage" d'un bit consiste à faire passer électriquement un élément binaire de la mémoire qui était à l'état logique "1" correspondant au crédit d'une unité à l'état logique "0" correspondant à un crédit nul. La mémoire de données étant réalisée en technologie "EPROM", ce changement d'état est électriquement irréversible.

Ces cartes à mémoire, appelées encore "cartes à puce" ont été décrites dans leur fonctionnement et leurs applications dans un article de Michel UGON et louis GUILLOU intitulé "les cartes à puce" publié dans la revue "La Recherche" n°176, avril

1986, vol.17, pages 472-479.

Bien que déjà très satisfaisants à certains égards, ces procédés de paiement électronique présentent cependant des inconvénients. En effet, d'une part, il n'est pas possible de recharger la carte, et d'autre part, la consommation de bits est élevée : le nombre de bits grillés est en effet égal au nombre de jetons à débiter.

Le but de l'invention est de remédier à ces inconvénients, en proposant un procédé dans lequel on peut recharger la mémoire pour recréditer celle-ci et dans lequel il suffit de griller un seul bit pour débiter n'importe quel nombre d'unités dans les limites du crédit disponible.

La possibilité de recharger la carte a conduit l'inventeur à désigner son système sous une forme imagée par l'expression "tirelire électronique".

Le procédé de l'invention est très simple et consiste en ceci. Une mémoire EPROM comprend des cellules binaires de mémorisation dont le contenu est égal soit à 0 soit à 1. Chaque cellule peut être grillée électriquement en faisant passer irréversiblement son contenu de l'état 1 à l'état 0. Le procédé de l'invention est caractérisé par le fait que les cellules de mémorisation sont groupées en entités qu'on appellera "éléments", chaque élément étant constitué d'au moins deux cellules de mémorisation. Chaque élément est repérable dans la mémoire par une adresse et il possède une parité : un élément est dit pair lorsque le nombre de ses cellules à l'état 1 est pair et il est dit impair lorsque le nombre de ses cellules à l'état 1 est impair.

Selon l'invention, le solde de la carte est égal au nombre d'éléments pairs non nuls dont l'adresse est inférieure à l'adresse de l'élément impair qui a la plus faible adresse. Ce dernier est appelé "borne". Si cet élément n'existe pas (ce qui est le cas avant le premier débit) le nombre d'éléments pairs non nuls est égal au nombre total d'éléments non nuls de la mémoire.

Pour débiter la carte et réduire le solde, on déplace

la borne vers une adresse plus basse en créant un nouvel élément impair d'adresse plus faible que le précédent. Ce nouvel élément impair devient donc la nouvelle borne. Le nombre d'unités débitées est égal au nombre d'éléments pairs non nuls situés entre l'ancienne borne et la nouvelle, plus 1.

Pour créditer la carte et augmenter le solde de celle-ci, on déplace la borne vers une adresse plus haute, en redonnant aux éventuels éléments déjà impairs d'adresse supérieure à la borne à déplacer, un caractère pair. Cela s'obtient en grillant une autre cellule de ces éléments. On crée aussi un nouvel élément impair d'adresse plus haute. Il se peut d'ailleurs que le rechargement soit tel que la nouvelle borne corresponde à un élément qui est déjà impair, auquel cas cet élément est laissé en l'état. Le nombre d'unités crédité dans la carte est égal au nombre d'éléments pairs non nuls situés entre l'ancienne borne et la nouvelle, plus 1.

Les éléments de mémorisation peuvent être des paires de cellules, ou des quartets ou des octets, ou des mots plus complexes. Dans une même mémoire, on peut trouver des éléments de structures différentes (par exemple des quartets associés à des octets).

De préférence, la carte est du type à microprocesseur (cartes dites "à puce") cartes qui existent déjà pour les applications visées plus haut. La mémoire de ces cartes comprend une (ou plusieurs) zone(s) réservée(s) constituée(s) d'octets et associée chacune à une autorisation, l'octet de base d'adresse A et l'octet suivant d'adresse A+1 n'étant pas disponibles pour le paiement, mais les octets d'adresse A+2 jusqu'à une adresse maximum Amax sont utilisables.

De toute façon, les caractéristiques de l'invention apparaîtront mieux à la lumière de la description qui suit, d'exemples de réalisation donnés à titre explicatif et non limitatif. Cette description se réfère à des dessins annexés sur lesquels :

- la figure 1 représente schématiquement l'état initial

d'une mémoire ne contenant que des "1",

- la figure 2 représente une première opération de paiement,
- la figure 3 représente une deuxième opération de paiement,
- la figure 4 repésente une première opération de rechargement,
- la figure 5 représente une deuxième opération de rechargement,
- la figure 6 représente une troisième opération de rechargement,
- la figure 7 représente une troisième opération de paiement,
- la figure 8 représente une quatrième opération de rechargement,
- la figure 9 représente schématiquement la répartition des différents mots d'une mémoire telle qu'on les trouve dans les cartes à puce classiques de type "porte-clés de contrôle d'accès",
- la figure 10 représente un organigramme montrant les diverses opérations impliquées dans la phase de rechargement,
- la figure 11 représente un organigramme montrant les diverses opérations impliquées dans la phase de paiement.

Dans la description qui suit, on supposera, à titre purement explicatif, que les éléments utilisés sont des quartets, c'est-à-dire des groupes de 4 cellules binaires. On ne fera par ailleurs aucune hypothèse sur la structure des circuits entourant la mémoire, ceux-ci pouvant être du type de ceux qu'on trouve dans les cartes actuelles dites "à puce", auxquels cas, ces circuits sont capables de remplir bien d'autres fonctions que celle de la gestion de la mémoire (émission de codes, chiffrement, déchiffrement, etc...) ; mais ces circuits peuvent être aussi d'un type plus simple, et plus spécifique de l'application "tirelire".

La figure 1 représente schématiquement les éléments

d'une mémoire avant utilisation. Toutes les cellules binaires sont chargées à 1. Tous les quartets sont donc pairs puisqu'ils contiennent tous quatre 1. Le solde initial So correspond au nombre de ces éléments. Ceux-ci sont repérés par une adresse qui va de A1 pour le premier, à Amax pour le dernier. Le quartet Amax constitue en quelque sorte le "fond" de la tirelire. On peut considérer que le premier élément impair est un quartet fictif qui serait à l'adresse fictive Amax+1.

La figure 2 représente schématiquement une première opération de paiement P de 4 unités. Le quatrième quartet avant le dernier (celui-ci compris), c'est-à-dire celui qui possède l'adresse Amax-3, est mis dans l'état impair, par grillage de l'un de ses bits, par exemple celui qui a le poids le plus faible. Le quartet d'adresse Amax-3 constitue alors une borne et le nouveau solde S1 est égal à So-4, qui est le nombre d'éléments pairs d'adresse inférieure à l'élément impair de plus faible adresse.

La figure 3 repésente schématiquement une deuxième opération de paiement Q de 2 unités. La borne est déplacée de deux rangs, en donnant au quartet d'adresse Amax-5 un caractère impair. C'est maintenant ce quartet qui est l'élément impair d'adresse la plus basse. Naturellement, le quartet d'adresse Amax-3 n'est pas modifié et reste impair. Après cette seconde opération, le nouveau solde est S2=S1-2.

Les opérations de paiement peuvent ainsi se succéder selon le même principe, la borne reculant vers des adresses de plus en plus basses.

Inversement, pour recharger la carte, on déplace la borne vers une adresse haute. La figure 4 représente ainsi un rechargement R d'une unité. Le quartet d'adresse Amax-5 est remis à l'état pair par grillage d'un second bit, ce qui équivaut à effacer la borne, et le quartet d'adresse Amax-4 est mis à l'état impair. C'est lui qui est alors le nouveau quartet impair de plus basse adresse et c'est donc lui qui constitue la nouvelle borne. Le solde passe de S2 à S3=S2+1.

La figure 5 montre un nouveau cas de rechargement S d'une unité. Le quartet d'adresse Amax-4 est mis à l'état pair par grillage d'un second bit, mais le quartet d'adresse Amax-3 est laissé intact car il se trouve déjà à l'état impair du fait de la première opération de paiement. Le solde passe de S3 à S4=S3+1.

La figure 6 montre encore un autre cas de rechargement T de 3 unités qui recharge la carte à S5=S4+3.

On peut à nouveau considérer des opérations de paiement : la figure 7 montre un paiement U de 4 unités qui conduit à redonner au quartet d'adresse Amax-4 un caractère impair, de sorte que cet élément contient maintenant trois 0 puisque c'est la troisième fois qu'il joue le rôle de borne. Si une opération V de rechargement intervient alors, il faut remettre ce quartet dans un état pair en grillant son dernier bit. Ce quartet ne contenant plus que des 0, il ne sera plus pris en compte par la suite. Le nouveau solde sera alors S7=S6+1 (bien que la borne ait été déplacée de deux rangs, car il est apparu un élément nul dans l'intervalle).

Le processus peut se poursuivre tant qu'il existe des quartets non nuls. Le solde maximum disponible se réduit peu à peu du fait de l'apparition d'éléments dont les bits sont tous nuls.

Il est clair qu'une opérationn de paiement n'est pas toujours possible : si le montant à prélever excède le solde, le paiement est impossible. De même, une opération de rechargement n'est pas toujours possible : si le montant à recharger excède la différence entre le nombre total d'éléments de la mémoire et le solde avant rechargement, celui-ci ne sera pas possible. Au mieux, on peut placer la borne dans un quartet fictif qui serait situé juste après le dernier quartet d'adresse Amax. Ainsi, l'opération de rechargement de la figure 6 ne pourrait porter au maximum que sur 4 unités. Dans ce cas, il n'y aurait plus de quartet impair dans la mémoire et l'on retrouverait un solde maximum So qui serait celui de l'étape initiale (figure 1). On

peut donc recharger "à bloc" la tirelire.

Il va de soi que, dans la pratique, les rechargements de la carte ne porteront pas, sauf exception, sur des montants aussi faibles que ceux qui viennent d'être envisagés et qui ont été choisis uniquement pour simplifier les explications. Dans la pratique, on opèrera des chargements de 50 ou de 100 unités par exemple.

Par ailleurs, en général, on procédera à une série de paiements puis à un seul rechargement, puis à une nouvelle série de paiements. La succession des trois rechargements R, S, T des figures 4, 5 et 6 n'était destinée qu'à illustrer différents cas de figure que l'on peut rencontrer dans la pratique, lors du rechargement (quartets déjà impairs, nuls, etc...).

Il va de soi aussi que la structure en bande continue de la mémoire, telle qu'elle apparaît sur les figures 1 à 8, n'est qu'une représentation schématique. Si l'on utilise une carte à puce telle que celles qui sont aujourd'hui en service du type porte-clés de contrôle d'accès, on peut y associer une zone de consommation à une autorisation. Cette zone de consommation est en fait organisée comme représenté sur la figure 9. Elle comprend jusqu'à 32 mots formés chacun de 4 octets. Pour des raisons de cohérence, ces mots commencent par le quartet 0110. L'octet de base d'adresse A contient un premier quartet égal à 0110, puis un second quartet constitué par un indicateur d'ouverture io et indicateur de fermeture if. L'octet suivant, d'adresse A+1 donne l'adresse maximum Amax relative au dernier octet de la mémoire.

Le premier mot n'offre donc que 2 octets disponibles. Les autres mots offrent chacun 1 quartet et 3 octets, soit 4 éléments. Au total, on dispose donc au maximum de 2+31x(1+3)=126 éléments, parmi lesquels 31 quartets et (2+31x3)=95 octets. La zone réservée comprend donc 31x4+95x8 soit 884 cellules binaires de mémorisation.

Si l'on utilisait le mode de paiement traditionnel par jetons, on disposerait donc, avec une telle mémoire, de 884

unités. Avec le procédé de l'invention, on peut disposer d'un nombre beaucoup plus grand d'unités.

En effet, au départ, on dispose de 126 unités (les 126 éléments). Après un certain nombre N de paiements, (dont le montant global ne doit pas excéder 126 unités), on peut recharger à bloc la mémoire en rendant pairs les N éléments ayant servi de bornes au cours des N paiements. On dispose donc à nouveau de 126 unités et l'on peut effectuer M paiements. Une recharge à bloc est encore possible en rendant pairs les M éléments ayant servi de bornes. Certains de ces éléments pourront avoit été rendus deux fois pairs et contiendront alors quatre 0 et ne seront plus pris en compte par la suite.

Naturellement, il arrive un moment où tous les éléments sont pairs, ce qui vide définitivement la tirelire, sans possibilité de rechargement.

Avec des réapprovisionnements fixes de 50 unités séparés par 20 paiements en moyenne, la zone peut être réapprovisionnée environ 16 fois, et porte donc de l'ordre de 800 unités. Ainsi, à 2,5 unités en moyenne par paiement, la consommation en tirelire a une efficacité comparable à la consommation par jetons en usage dans les cartes actuelles.

Mais avec des réapprovisionnements fixes de 100 unités et des paiements moyens de 20 unités, le procédé de l'invention permettra des transactions portant sur environ 7000 unités. On saisit alors tout l'intérêt du procédé.

La figure 10 est un organigramme illustrant les opérations effectuées lors d'un rechargement. Dans cet organigramme, la signification des opérations repésentées conventionnellement par des rectangles ou des losanges est la suivante :

100 : introduction à l'opération de chargement de la carte ; définition de l'adresse de base A et du nombre d'unités K à charger. La variable j donnera à la fin le nombre d'unités effectivement chargées,

102 : lecture de l'élément d'adresse A+1 donnant l'adresse Amax

fixant le fond de la zone réservée et initialisation de j à 0 et d'un indice courant i à 2. Par ailleurs, une variable logique binaire qu'on peut appeler "borne", est créée qui peut prendre une valeur 0 signifiant qu'on recherche la borne et une valeur 1 signifiant qu'on a trouvé la borne,

104 : lecture de l'élément d'adresse A+i, soit A+2 au départ,

105 : l'élément d'adresse A+i est-il pair ?

106 : l'élément d'adresse A+i, qui est pair, est-il nul ?

107 : la borne est trouvée (la variable logique est mise ou laissée à l'état 1).

108 : la borne est-elle trouvée ?

110 : l'indice i est-il à son maximum (c'est-à-dire l'adresse A+i est-elle égale à l'adresse maximum Amax) ?

112 : augmenter i d'une unité,

114 : j est-il égal à K, autrement dit le nombre j d'unités dénombrées est-il égal au nombre souhaité K ?

116 : j est-il égal à K ?

118 : augmenter j d'une unité,

120 : griller un bit dans l'élément d'adresse A+i,

122 : j est-il égal à K ?

124 : retour au programme principal, j unités ayant été introduites sur les K demandées.

La figure 11 représente, de la même manière, un organigramme illustrant les opérations effectuées lors d'un paiement. Les opérations référencées ont la signification suivante :

200 : introduction à l'opération de paiement ; définition de l'adresse de base A, du nombre d'unités K à débiter. La variable indiquera à la fin le solde j au cas où il serait insuffisant, c'est-à-dire inférieur à K,

202 : lecture de l'élément d'adresse A+1 donnant l'adresse Amax fixant le fond de la zone réservée et initialisation de j à 0 et d'un indice courant i à 2,

204 : lecture de l'élément d'adresse A+i,

205 : l'élément lu est-il pair ?

206 : i est-il maximum ?

208 : augmenter i d'une unité,

210 : j est-il égal à K ?

212 : l'élément d'adresse A+i est mis ou laissé à l'état impair et retour au programme général,

214 : i est-il égal à 2 ?

216 : diminuer i d'une unité,

218 : lire l'élément d'adresse A+i,

220 : augmenter j d'une unité,

222 : le solde est insuffisant pour débiter K unités ; retour au programme général. Dans ce cas, la variable j indique le solde.

Il va de soi que c'est par pure convention que l'on a supposé que la mémoire contenait initialement des "1". On aurait pu tout aussi bien convenir qu'il s'agissait de 0, l'essentiel étant que l'opération de grillage fasse passer irréversiblement une cellule d'un certain état binaire à l'autre état binaire.

Il est clair également qu'on peut commencer par griller n'importe quel bit dans un élément pour rendre ce dernier impair, et qu'il n'est pas nécessaire d'agir d'abord sur le bit de plus faible poids. Ceci montre clairement un autre avantage du procédé. Pour réaliser une opération de paiement, on a toujours le choix entre au moins deux bits. Par conséquent, en cas de difficultés pour écrire la mémoire, ce qui arrive parfois, on dispose d'une solution très simple de rechange.

Naturellement, on pourrait inverser aussi les parités et partir d'une mémoire à éléments tous impairs. La borne serait alors le premier élément pair. Mais dans la pratique il semble plus commode de partir d'éléments pairs que l'on rend impairs.

REVENDICATIONS

1. Procédé de paiement électronique utilisant une carte à mémoire EPROM comprenant des cellules binaires de mémorisation ayant un contenu logique égal soit à 0 soit à 1, chaque cellule pouvant être grillée électriquement en faisant passer irréversiblement son contenu d'un état à un autre, ce procédé étant caractérisé par le fait que :

- les cellules de mémorisation sont groupées en éléments groupant au moins deux cellules, chaque élément étant repérable par une adresse et ayant une parité, un élément étant dit pair lorsque le nombre de ses cellules à l'état 1 est pair et dit impair lorsque le nombre de ses cellules à l'état 1 est impair,

- le solde de la carte est le nombre d'éléments non nuls ayant une première parité et d'adresse inférieure à l'adresse de l'élément de parité opposée qui a la plus faible adresse et qui est appelée "borne", ou, si cet élément n'existe pas, le nombre d'éléments de cette première parité non nuls de la mémoire,

- pour débiter la carte et réduire ce solde, on déplace la borne vers une adresse plus basse en créant un nouvel élément de parité opposée d'adresse plus faible que la borne à déplacer, ce nouvel élément devenant la nouvelle borne, le nombre P d'unités débité étant égal au nombre d'élément de première parité situé entre l'ancienne borne et la nouvelle, plus 1,

- pour créditer la carte et augmenter ce solde, on déplace la borne vers une adresse plus haute, en redonnant aux éventuels éléments ayant déjà ladite parité opposée et ayant une adresse supérieure à la borne à déplacer la première parité et cela en grillant une nouvelle cellule et en créant un nouvel élément ayant la seconde parité, d'adresse plus haute que la borne à déplacer, à moins que cet élément ait déjà cette parité, auquel cas il est laissé tel quel, le nombre K d'unités crédité dans la carte étant égal au nombre d'éléments ayant la première

parité situés entre l'ancienne borne et la nouvelle, plus 1.

2. Procédé selon la revendication 1, caractérisé par le fait que la première parité est la parité paire et la parité opposée la parité impaire, la borne étant constituée par l'élément impair de plus basse adresse.

3. Procédé selon la revendication 1, caractérisé par le fait que les éléments de mémorisation peuvent être soit des paires, soit des quartets, soit des octets, soit des mots plus complexes, soit une combinaison de ces divers éléments.

4. Procédé selon la revendication 1, caractérisé par le fait que la carte est du type à microprocesseur avec une mémoire comprenant une zone réservée constituée d'octets, l'octet de base d'adresse A et l'octet suivant d'adresse A+1 n'étant pas disponibles pour le paiement, la zone réservée aux paiements et aux rechargements allant de l'octet d'adresse A+2 au dernier octet d'adresse Amax.

5. Procédé selon la revendication 3, caractérisé par le fait que la zone réservée comprend M mots constitués de N octets chacun, chaque mot commençant par un premier octet dont le quartet de poids fort est déterminé et le même pour tous les mots, les éléments utilisables pour le paiement étant ainsi constitués par le quartet de poids faible qui appartient au premier octet de chaque mot, et les octets suivants de chaque mot.

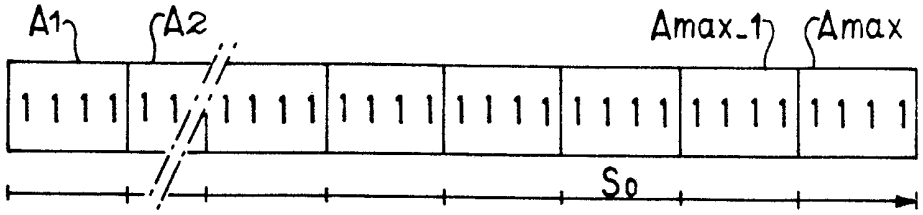


FIG. 1

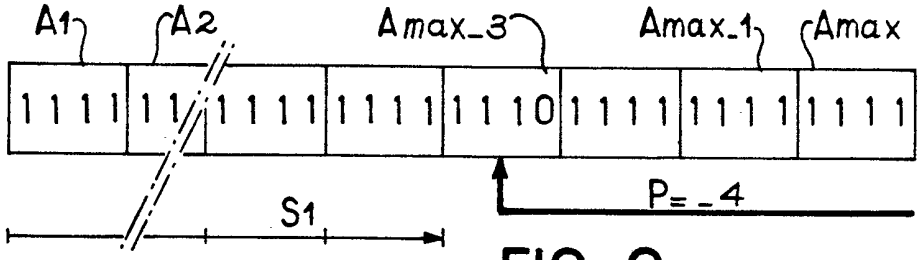


FIG. 2

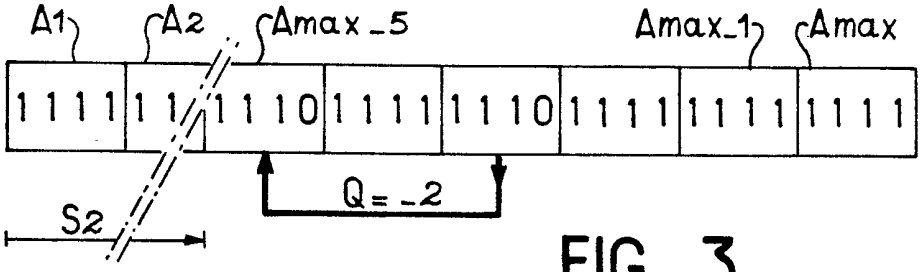


FIG. 3

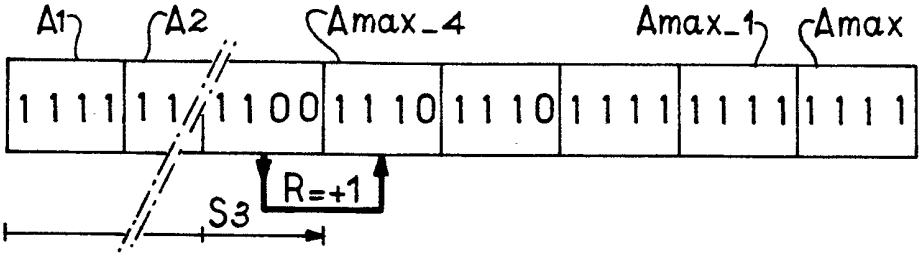


FIG. 4

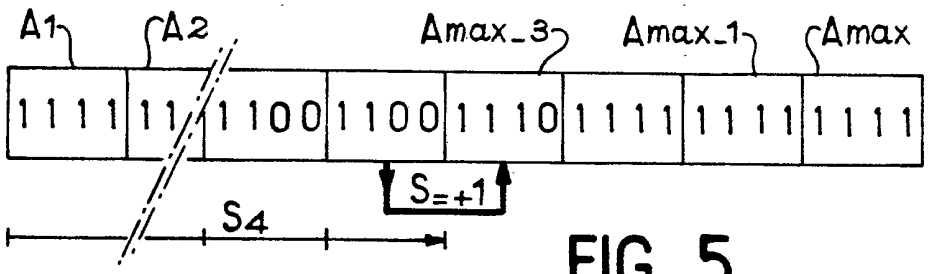


FIG. 5

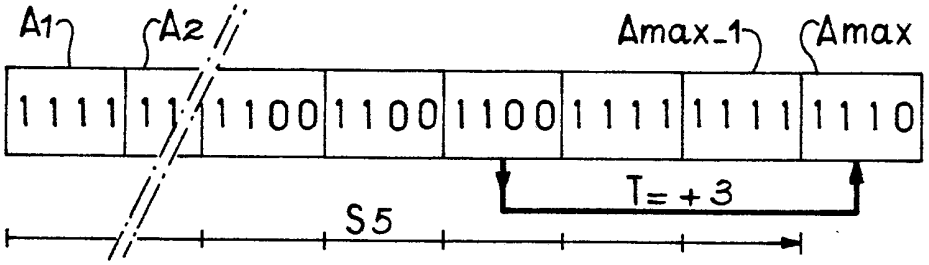


FIG. 6

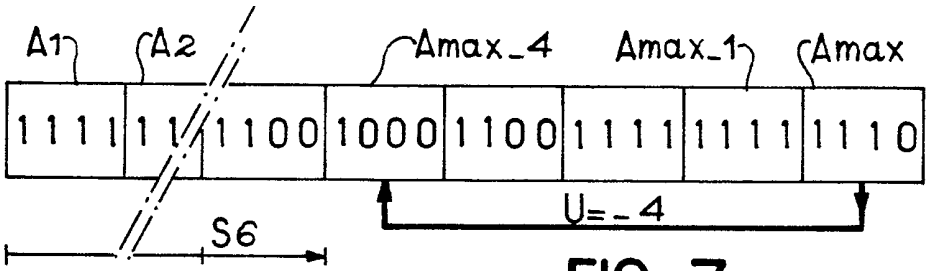


FIG. 7

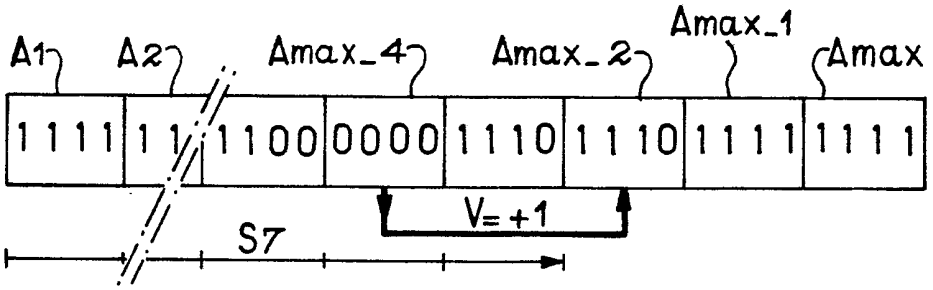


FIG. 8

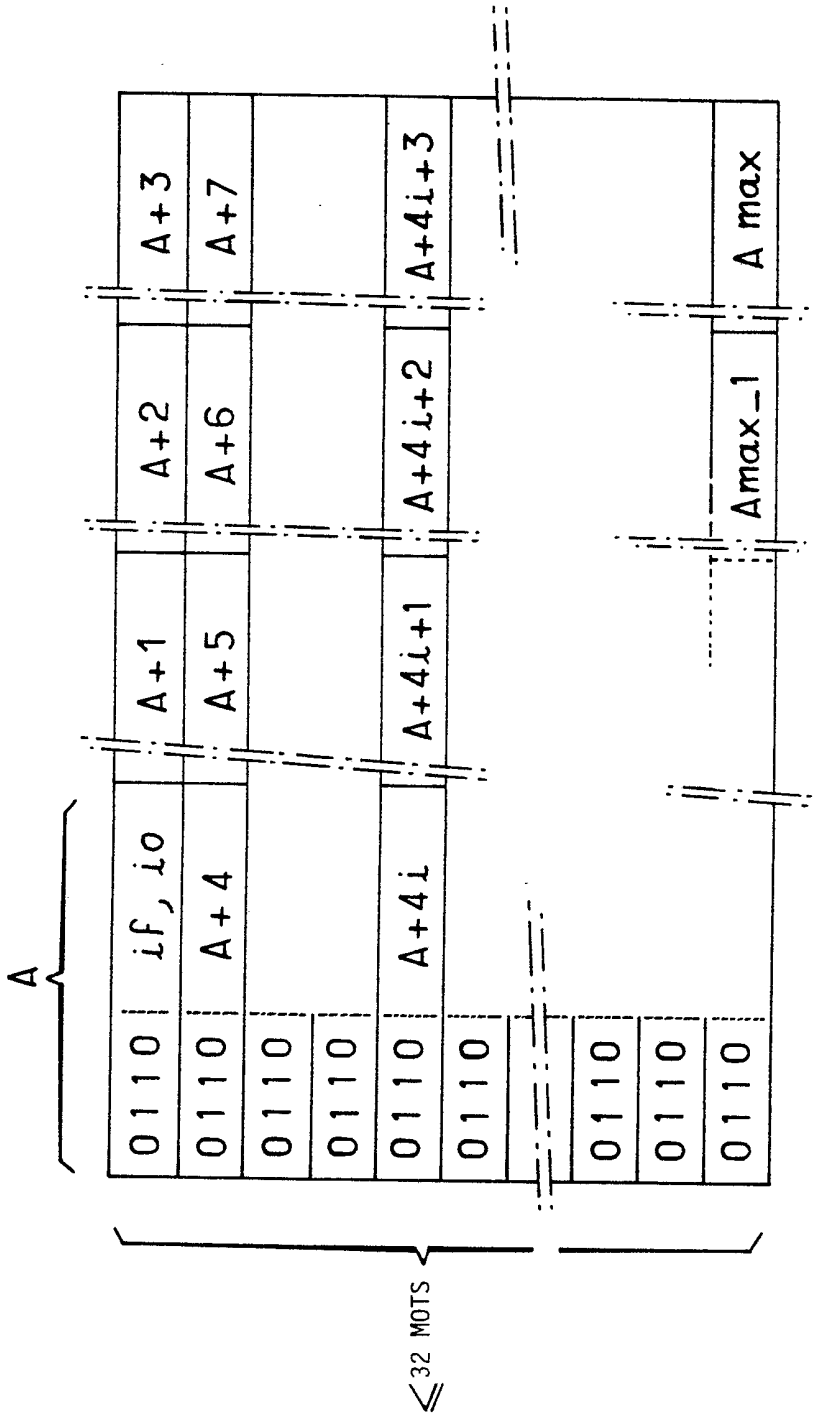

A
if, io
A+4
A+4i
A+1
A+5
A+4i+1
A+2
A+6
A+4i+2
A+3
A+7
A+4i+3
A max
Amax_1
0110
≤32 MOTS

FIG. 9

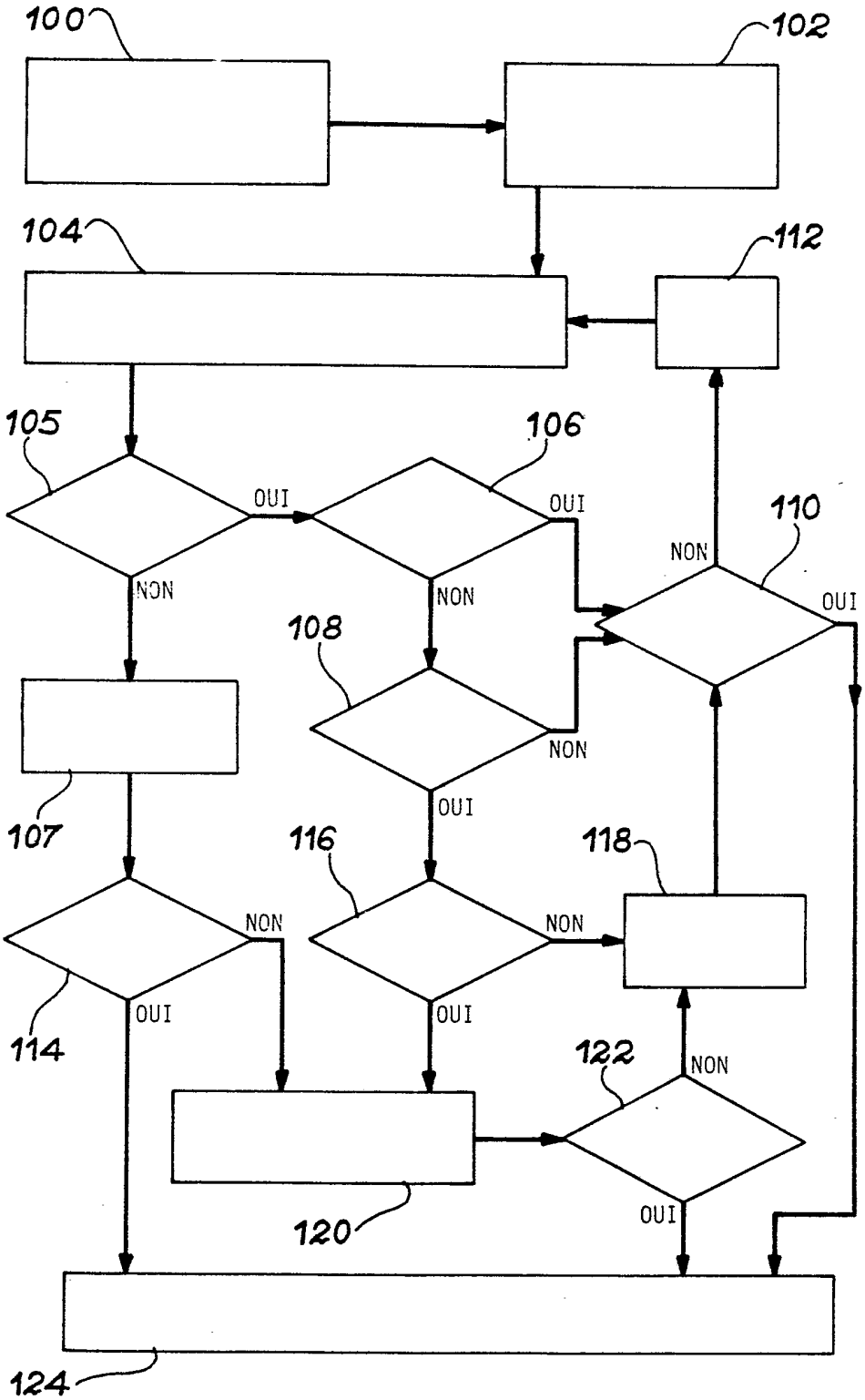

100
102
104
112
105
106
OUI
OUI
NON
NON
110
NON
OUI
108
NON
OUI
107
116
118
NON
NON
OUI
OUI
114
122
NON
120
OUI
124

FIG. 10

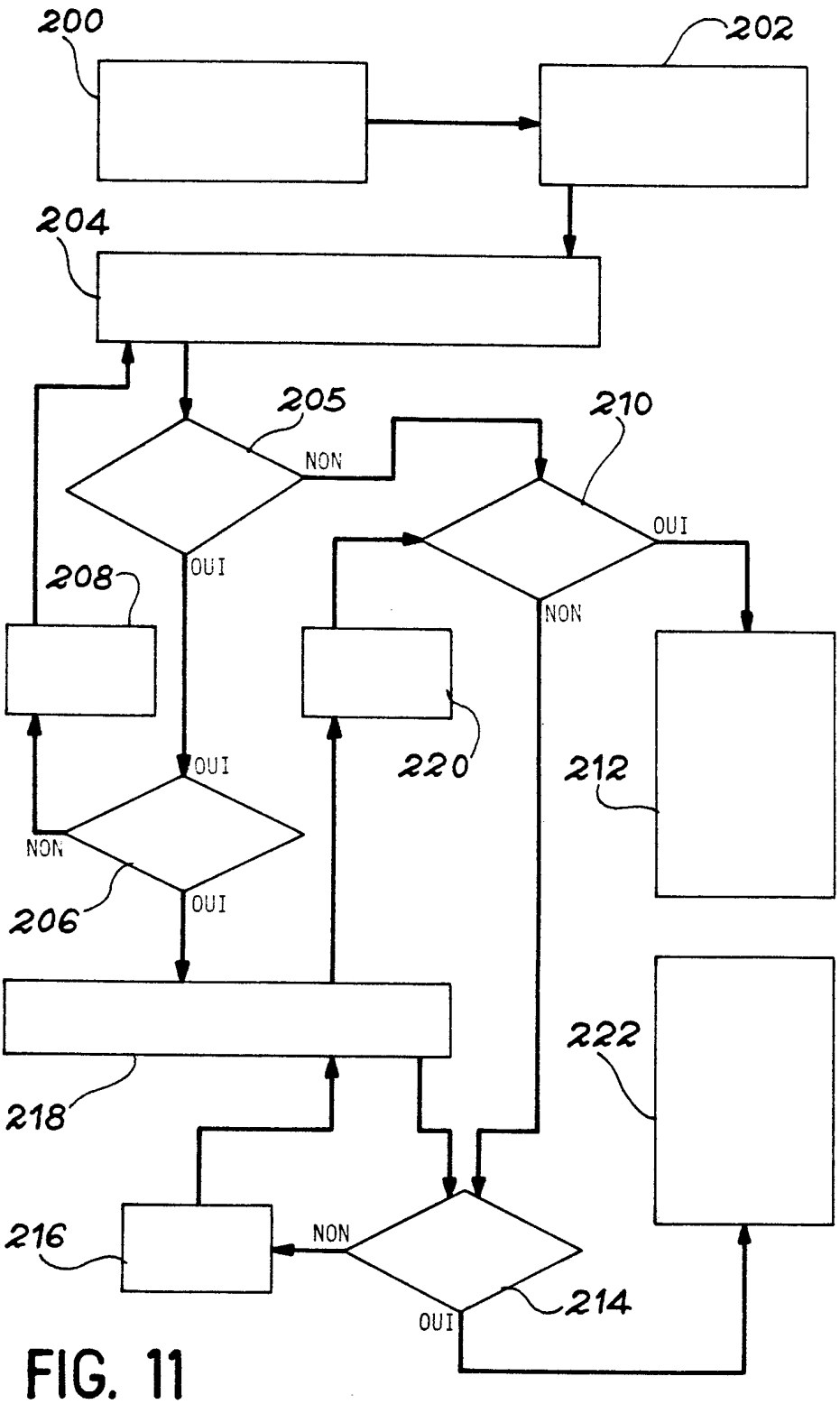

200
202
204
205
NON
OUI
210
OUI
NON
208
OUI
220
212
NON
OUI
206
218
222
216
NON
214
OUI

FIG. 11