(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

ROMÂNIA

(11) **RO 128241 A2**
(51) Int.Cl.
G06Q 20/00 (2006.01);
G06Q 90/00 (2006.01);
G06F 17/00 (2006.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2011 00828**

(22) Data de depozit: **23.08.2011**

(41) Data publicării cererii:
29.03.2013 BOPI nr. **3/2013**

(71) Solicitant:
• **UNIVERSITATEA "BABEŞ-BOLYAI" DIN CLUJ-NAPOCA**,
STR.MIHAIL KOGĂLNICEANU NR.1, CLUJ-NAPOCA, CJ, RO

(72) Inventatori:
• **DUMITRU DUMITRESCU**, *STR. DONAT NR. 109, AP. 36, CLUJ-NAPOCA, CJ, RO;*
• **BARTHA ATTILA**, *STR. TINERETULUI NR. 9/13, ODORHEIU SECUIESC, HR, RO;*
• **CREMENE MARCEL**, *STR. ZORILOR NR. 36, CLUJ NAPOCA, CJ, RO*

(54) # PROCEDEU PENTRU REZOLVAREA PROBLEMEI NP-COMPLETE "SUBSET-SUM"

(57) **Rezumat:**

Invenţia se referă la un procedeu ce permite rezolvarea unei probleme "subset-sum", din domeniul teoriei complexităţii computaţionale, nerezolvabilă în timp polinomial determinist, cu aplicaţii în criptografie şi optimizare. Procedeul conform invenţiei foloseşte un ansamblu numit sistem cascadă, bazat pe semnale electrice binare, discret în timp şi sincron, format dintr-un nod sursă S (**1**), o serie de module M_j (**2**), ce conţin celule (**5**) de întârziere şi porţi logice (**6**) de tip SAU, şi un nod de test T (**3**), sursa S (**1**) generează un impuls treaptă, ce se transmite la intrarea lanţului de module M_j (**2**) de prelucrare a semnalelor de la intrarea acestora, în vederea calculului sumelor parţiale, modulele M_j (**2**) ale sistemului corespund numerelor din mulţimea de numere dată, fiecare extinzând rezultatul parţial de la intrarea sa, prin adăugarea soluţiilor parţiale corespunzătoare numărului reprezentat de către modulul respectiv, iar nodul de test T(**3**) este amplasat la ieşirea sistemului, având rol de a verifica dacă soluţia căutată se află printre soluţiile generate de sistem, adică dacă starea logică la ieşirea ultimului modul M_i este "1" logic la un moment de timp discret egal cu suma "sum" ce se doreşte a fi verificată.

Revendicări: 4
Figuri: 2

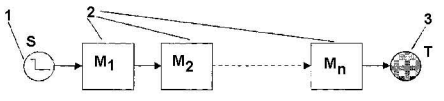

Fig. 1

RO 128241 A2

OFICIUL DE STAT PENTRU INVENȚII ȘI MĂRCI
Cerere de brevet de invenție
Nr. a 2011 00828
Data depozit 23 -08- 2011

Procedeu pentru rezolvarea problemei NP complete „subset-sum"

Invenția se referă la un procedeu ce permite rezolvarea problemei „subset-sum". În informatică, problema „subset-sum" este o problemă clasica importantă în domeniul *teoriei complexității computationale* cu aplicatii in *criptografie si optimizare*.

Problema se defineste astfel: dându-se o multime de numere întregi pozitive şi un număr *sum* se cere să se verifice dacă există o submulțime nevidă a acestei multimi astfel incât suma elementelor acesteia să fie egală cu numărul *sum*.

Problema „subset-sum" este NP-completă (nerezolvabilă în timp polinomial determinist). Multe probleme NP-complete de optimizare combinatorială pot fi reduse la această problemă. Se cunosc scheme criptografice bazate pe „subset-sum". Existența unui procedeu rapid de rezolvare a problemei poate fi utilizată în decriptarea mesajelor care folosesc scheme criptografice de acest tip. Procedeul propus poate fi generalizat şi utilizat în rezolvarea unor probleme dificile (NP-complete) de optimizare combinatorială şi de criptografie.

Problemele practice de optimizare la care poate fi aplicata inventia sunt de tip „bin packing". Procedeul propus are aplicabilitate în solutionarea problemelor de alocare eficientă de resurse cum ar fi: decuparea materialelor cu pierderi minime, împachetarea unor obiecte într-un container, alocarea optimă a timpilor de executie a unor procese, utilizarea optimă a spațiilor de transport sau depozitare şi altele.

În scopul găsirii rapide a unor soluții la probleme NP-complete în general nu se cunoaste nici o modalitate eficientă de rezolvare. Timpul necesar pentru a rezolva acest tip de probleme folosind algoritmi cunoscuti creşte foarte repede atunci când dimensiunea problemei creşte. Versiuni moderat de mari ale unora dintre problemele NP-complete necesită timpi de calcul de ordinul a miliarde de ani, folosind puterea de calcul disponibila astăzi. Ca o consecință, a determina dacă este sau nu posibil să rezolvăm aceste probleme mai repede, adică a rezolva problema P (polinomial) versus NP (non-polinomial) este una dintre principalele *probleme nerezolvate* în stiinta calculatoarelor de azi.

În scopul rezolvării problemei „subset-sum", metoda clasică este reprezentată de un algoritm de programare dinamica specific. Acest algoritm rulează în timp pseudo-polinomial şi foloseste o cantitate de memorie proportională cu *N* înmultit cu valoarea *sum*, unde *N* este cardinalul multimii numerelor din problemă. Aceasta metodă însă se bazează pe o implementare software. Este dificil de paralelizat şi de implementat hardware. Acest algoritm este descris în lucrări cum sunt: Cormen, Thomas H.; Leiserson, Charles E., Rivest, Ronald L., Stein, Clifford (1990), *The subset-sum problem. Introduction to Algorithms*, MIT Press and McGraw-Hill, şi Michael R. Garey, David S. Johnson (1979), *Computers and Intractability: A Guide to the Theory of NP-Completeness.*

În acelasi scop, al rezolvării problemei „subset-sum", se mai cunoaste o metodă bazată pe sisteme de tip "Spiking Neural P Systems". Astfel de sisteme rezolvă problemă subset-sum prin procesare paralelă, ceea ce conduce la un timp de rezolvare acceptabil. Dezavantajul acestei metode constă în faptul că numărul de componente necesare creşte exponential cu cardinalul multimii numerelor din problema şi deci prezintă o complexitate spatială exponentială. Aceasta abordare este tratată în lucrarea: A. Leporati, M. A. Gutiérrez-Naranjo, *Solving SUBSET SUM by Spiking Neural P Systems with Pre-computed Resources*, în Fundamenta Informaticae, Vol. 87 Issue 1, pp. 61-77, (2008).

În acelasi scop, mai este cunoscută de asemenea o metodă bazată pe abordarea numită "Optical Computing". În această abordare solutia problemei „subset-sum" este găsită cu ajutorul unui sistem optic prin care se propaga impulsuri luminoase. Aceasta abordare este caracterizată printr-un timp de rezolvare redus. Complexitatea spatială este proportională cu cardinalul numerelor din problema subset-sum. Folosirea acestei metode în practică prezintă însă limitări importante datorate costurilor de implementare a sistemelor optice, scăderii exponentiale a amplitudinii impulsurilor luminoase de-a lungul sistemelor optice prin care se propaga acestea, dificultătilor tehnice care apar în detectarea şi separarea impulsurilor luminoase foarte scurte şi apropiate în timp. Această metodă este prezentată în lucrarea: M. Oltean, O. Muntean, *Solving the subset-sum problem with a light-based device*, Natural Computing, vol.8 no.2, pp.321-331, (2009).

Problema tehnică pe care o rezolvă inventia este găsirea unei solutii eficiente pentru problema NP-completa „subset-sum" care sa satisfacă următoarele cerinte:

- sa aibă timp de calcul si complexitate reduse, adecvata la situatii in care timpul si complexitatea spatiala sunt limitate;
- sa fie usor paralelizabila;
- sa fie facil implementabila hardware;
- sa aibă costuri de implementare reduse.

Procedeul de rezolvare a problemei NP complete „subset-sum", conform inventiei, rezolvă problema „subset-sum" prin utilizarea unui ansamblu numit *sistem cascadă*, ilustrat în figura 1. Acest sistem este discret în timp şi sincron, bazat pe semnale electrice binare. Este format dintr-o sursa de semnal S (1), un nod terminal T (3) si mai multe module (2), ilustrate in figura 2. Modulele (2) contin la rândul lor celule de întârziere (5) şi porti logice de tip SAU (6).

Procedeul de rezolvare a problemei NP complete „subset-sum" se bazează pe sistemul cascadă descris în figura 1 şi constă în: generarea unui impuls treaptă la nodul sursa S (1), impuls ce se transmite la intrarea lantului de module (2). Acest lant de module este format dintr-un număr de n module M_j (2), ce au rolul procesării semnalelor de la intrarea acestora în vederea calculului sumelor partiale.

Modulele sistemului corespund numerelor din multimea de dată. Fiecare modul extinde rezultatul partial de la intrarea sa prin adăugarea solutiilor partiale corespunzătoare numărului reprezentat de către modulul respectiv. Modulele contin la rândul lor lanturi de celule de memorie (5) si porti logice de tip SAU (6).

De la iesirea fiecărui modul spre modulul următor se propagă semnale binare. Sistemul este discret în timp şi sincron: fiecare nod işi schimbă starea în mod sincron la momente de timp determinate.

Un nod de test T (3) este amplasat la iesirea sistemului având rolul de a verifica dacă solutia căutată se află printre solutiile generate de sistem. Pentru aceasta, se verifică dacă starea logică a semnalului la iesirea sistemului este *„1"* logic la momentul temporal discret egal cu *sum*, adică după un timp egal cu *sum* perioade de tact ale sistemului discret. Dacă se verifică conditia înseamnă că valoarea *sum* poate fi calculată ca o sumă a unui subset de elemente al multimii de numere date, deci problema este rezolvată.

Se dă în continuare un exemplu de realizare a inventiei, în legătură cu figurile 1 şi 2 care reprezintă:

- Figura 1 – Arhitectura sistemului cascada ce implementează procedeul propus;
- Figura 2 – Structura interna a unui modul M_j din arhitectura sistemului cascada.

Atât in figura 1 cat şi în figura 2 liniile şi săgetile semnifică conexiuni iar sensul săgetilor indică sensul propagării semnalelor binare.

In figura 1 este descris un sistem cascada care reprezintă o modalitate de realizare a invenţiei. Sa presupunem că multimea de numere întregi pozitive dată este $A = \{e_1, e_2, \ldots e_n\}$. Sistemul cascadă are o structură liniară şi este bazat pe prelucrări succesive de semnal. Sistemul este unul binar, lucrând in timp discret, pe baza unui semnal de tact. In starea initială toate nivelele de semnal din sistem sunt în starea „*0*" logic.

Sistemul cascadă (fig. 1) este compus din următoarele elemente:

- Un nod sursa S (1) ce reprezintă o sursă binară ce generează un semnal treapta (iesirea nodului este in starea logica „*1*" pe durata primul impuls de tact si „*0*" in rest).
- Un număr de n module M_j (2) ce au rolul procesării semnalelor de la intrarea acestora in vederea calculului sumelor partiale.
- Pentru fiecare element e_j din multimea A va exista un modul M_j. Prin urmare, numărul total n de module este egal cu numărul de elemente ale multimii A. Structura interna a unui nod de tip M_j este descrisa in figura 2 si va fi detaliata mai jos.
- Nodul de test T (3) are rolul de a verifica solutiile problemei. Acest nod verifica daca la un moment de timp dat t_{test} starea iesirii ultimului bloc de procesare, M_n, este in „*1*" logic. Pentru a verifica daca exista o sub-multime a multimii A având proprietatea ca suma elementelor este egală cu *sum* este suficient să se seteze timpul $t_{test} = sum$.

Fiecare modul M_j, descris în figura 2, are o intrare (4) respectiv o iesire (7) si este compus din următoarele elemente:

- Un lant de celule de întârziere $a_1 \ldots a_k$ (5) ce formează o linie de întârziere a semnalului cu k tacti. Un nod a_i întârzie semnalul de la intrarea sa cu un tact: iesirea nodului a_i este egala cu intrarea nodului a_i la momentul de timp anterior. Pentru fiecare modul M_j va exista un număr de k noduri a_i , $k = e_j$ din multimea A.
- O poarta logica de tip SAU (6).

Functionarea sistemului cascadă se explică astfel: dacă la momentul *t* intrarea unui modul M_i se află în starea *"1"*, datorită funcției SAU (6) iesirea va fi, de asemenea, în starea *"1"* la momentul *t* dar si la momentul $t+k$, unde *k* este numărul de celule de întârziere care este în acest caz egal cu e_i adică elementul *i* din multimea *A*. Acest lucru se explică prin faptul că valoarea *„1"* de la intrare ajunge la poarta SAU întârziata cu *k* tacți.

În cazul în care două module M_i şi M_{i+1} sunt concatenate, un semnal *„1"* prezent la momentul *t* la intrarea modulului M_i apare la iesirea lui M_{i+1}: la acelasi moment *t*, la momentul $t+e_i$, la momentul $t+e_{i+1}$ si la momentul $t+e_i+e_{i+1}$. Prin inductie, se demonstrează că momentele de timp la care apare un semnal de *„1"* la iesirea unui lant de module M_i sunt date de toate sumele partiale ale elementelor multimii A.

Complexitatea în timp a metodei propuse este egală cu o constanta *u* înmultită cu valoarea *sum* dată, deci este liniară în raport cu *sum*. Constanta *u* este egală cu perioada semnalului de tact al sistemului discret. Aceasta are valori tipice în jur de 10^{-9} secunde pentru sistemele hardware actuale.

Complexitatea spatială este dată de numărul total de celule de întârziere din sistemul cascada si este egală cu suma elementelor multimii *A* date. Aceasta mărime este de asemenea rezultatul unei combinatii liniare. Prin urmare, complexitatea spațială este de asemenea liniară în raport cu suma elementelor mulțimii *A*.

Prin utilizarea procedeului propus pentru rezolvarea problemei NP complete „subset-sum" se obțin următoarele avantaje:

- implementare hardware facila, spre deosebire de majoritatea algoritmilor existenti, care au fost conceputi pentru implementări software,
- viteza de lucru ridicata conferita de paralelismul intrinsec,
- permite rezolvarea intr-o singura rulare a tuturor problemelor „subset-sum" pentru valori *sum* mai mici sau egale cu o valoare data,
- complexitate in timp liniara in raport cu *sum*,
- complexitate spatiala liniara in raport cu suma elementelor multimii date,
- costuri si complexitate de implementare hardware reduse.

a-2011-00828--
23 -08- 2011

REVENDICĂRI

1. Procedeu pentru rezolvarea problemei NP-complete „subset-sum" **caracterizat prin aceea că** folosette un ansamblu numit sistem cascada, bazat pe semnale electrice binare, discret in timp si sincron, format din: un nod sursa S (1), o serie de module M_j (2) ce contin celule de întârziere (5) si porti logice de tip SAU (6), si un nod de test T (3).
2. Procedeu, conform revendicării 1 si 2, **caracterizat prin aceea că** sursa S (1) generează un impuls treapta ce se transmite la intrarea lantului de module M_j (2) de prelucrare a semnalelor de la intrarea acestora in vederea calculului sumelor partiale.
3. Procedeu, conform revendicării 1, 2 si 3, **caracterizat prin aceea că** modulele M_j (2) ale sistemului corespund numerelor din multimea de numere data, fiecare extinzând rezultatul partial de la intrarea sa prin adăugarea solutiilor partiale corespunzătoare numărului reprezentat de către modulul respectiv.
4. Procedeu, conform revendicării 1, 2, 3 si 4 **caracterizat prin aceea că** un nod de test T (3) este amplasat la iesirea sistemului, având rolul de a verifica daca solutia căutata se afla printre solutiile generate de sistem, adică daca starea logica la iesirea ultimului modul M_t este *„ 1"* logic la un moment de timp discret egal cu suma *sum* ce se doreste a fi verificata.

a-2011-00828--
23 -08- 2011

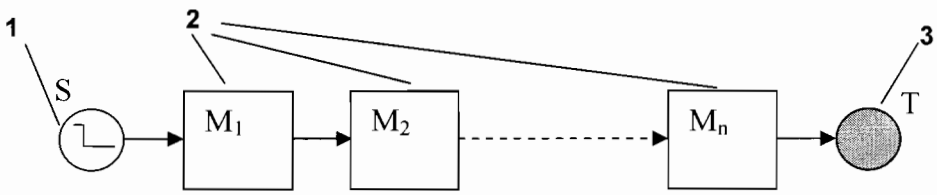

Figura 1

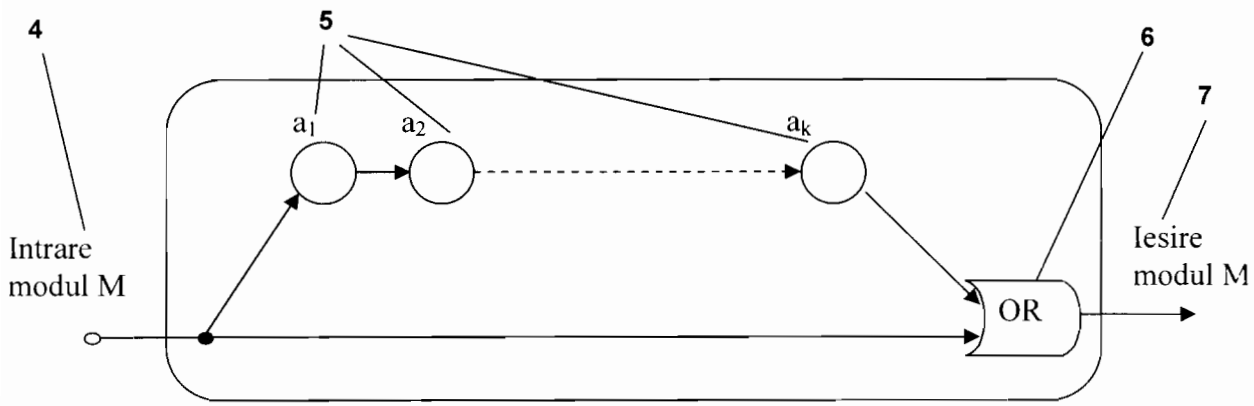

Figura 2