RAČUNARSTVO
Sveska 1, Broj 2, 1992

UDK 519.688

KUREPINA HIPOTEZA O LEVOM FAKTORIJELU[1]

GORAN GOGIĆ

SAŽETAK. Na kongresu jugoslovenskih matematičara u Ohridu 1970. godine Đuro Kurepa je postavio sledeći problem: definišimo levi faktorijel kao sumu faktorijela svih nenegativnih celih brojeva manjih od datog broja; postavlja se pitanje šta može biti zajednički delilac levog i desnog faktorijela nekog broja. Kurepa postavlja hipotezu da je dvojka najveći zajednički delilac oba ova broja. Mada je problem veoma jednostavan, i na prvi pogled se čini da ne bi trebalo biti nekih poteškoća pri rešavanju, on do danas, 20 godina od nastanka, nije rešen.

1 Neki iskazi ekvivalentni Kurepinoj hipotezi

U cilju pojednostavljenja problema, pojavili su se mnogi iskazi ekvivalentni iskazu Kurepine hipoteze. Iskaz (E1) koji Kurepa navodi u [5] biće nam od velike pomoći pri proveri (KH) na računaru.

DEFINICIJA 1. *Levi faktorijel prirodnog broja n (u oznaci !n) definišemo kao*

$$!n = \sum_{i=0}^{n-1} i! = 0! + 1! + \cdots + (n-1)!.$$

DEFINICIJA 2. *Kurepina hipoteza je iskaz*

$$(\mathrm{KH}) \qquad (\forall n > 1)\,\mathrm{NZD}(!n, n!) = 2$$

DEFINICIJA 3. *Neka je P skup prostih brojeva. Iskaz (E1) je*

$$(\mathrm{E1}) \qquad (p \in P)(p > 2 \Rightarrow !p \not\equiv 0 \ (mod p))$$

TEOREMA 1. *Iskazi (KH) i (E1) su ekvivalentni.*

[1]Rad finansiran od Fonda za nauku Republike Srbije preko Matematičkog instituta, projekat 0401A.

DOKAZ:

- $\neg(E1) \Rightarrow \neg(KH)$ Neka je $p \in P$ takav da je $p > 2$ i $!p \equiv 0 \pmod{p}$. Međutim, pošto je p prost, to znači da $p|!p$, a kako $p|p!$ onda je $\mathrm{NZD}(!p, p!) \geq p > 2$ i za $n = p$ dobijamo $\mathrm{NZD}(!n, n!) \neq 2$ što je negacija od (KH).
- $\neg(KH) \Rightarrow \neg(E1)$ Pošto je (KH) tačno za $n \leq 4$, to onda mora za neko $n > 4$ da važi $\mathrm{NZD}(!n, n!) = d$ i $d \neq 2$. Sada je

$$\begin{aligned} !n &= 0! + 1! + 2! + \cdots + (n-1)! \\ &= 10 + 4! + \cdots + (n-1)! \equiv 2 \pmod{4} \end{aligned}$$

a pošto $4|n!$ za $n > 4$, to onda $2|d$ i $4!d$ odakle je $d \neq 1$ a zbog $d \neq 2$ zaključujemo da d ima neki prost neparan delilac. Neka je $p > 2$ prost broj takav da $p|d$. Pošto $p|n! = 1 \cdot 2 \cdot \ldots \cdot n$ to je $p \leq n$. Međutim, $!n = !p + p! + (p+1)! + \cdots + (n-1)! \equiv !p \pmod{p}$ pa kako $p|!n$ to $p|!p$ što je u stvari negacija iskaza (E1). Ovim je teorema dokazana.

2 Opšta rekurentna formula

Pošto smo navedenom teoremom smanjili domen na kome treba ispitati tačnost (KH), ostaje da nađemo najlakši način za računanje vrednosti funkcije levog faktorijela.

TEOREMA 2. *Neka su funkcije* $\mathrm{V}: N \times N \to N$ *i* $\mathrm{W}: N \times N \to N$ *definisane na sledeći način:*

$$\mathrm{V}(n,k) = \prod_{i=0}^{k+1} (n-i) = n(n-1)\ldots(n-k+1) = n!/k!$$

$$\mathrm{W}(n,k) = \sum_{i=1}^{k} \mathrm{V}(n-i, k-i)$$

Neka su dalje dati prirodni brojevi k *i* n *pri čemu je* $k < n$ *i neka je* $l = [n/k]$ *i* r *takvo da je* $n = kl + r$, $0 \leq r < n$. *Ako je niz* S $(0 \leq i \leq l)$ *definisan na sledeći način:*

$$\begin{aligned} &S_0 = \mathrm{V}(n,k), \\ &S_i = S_{i-1} \cdot \mathrm{V}(n-ik, k) + \mathrm{W}(n-ik, k), \quad 1 \leq i < l, \\ &S_l = S_{l-1} \cdot r! + !r, \end{aligned}$$

tada je $S_l = !n$.

DOKAZ: Neka je $k \in N$ takvo da je $k < n$. Tada je

$$\begin{aligned} !n - !(n-k) &= \sum_{i=1}^{n}(n-i)! - \sum_{i=1}^{n-k}(n-k-i)! \\ &= \sum_{i=1}^{n}(n-i)! - \sum_{i=k+1}^{n}(n-i)! \\ &= \sum_{i=1}^{k}(n-i)!, \end{aligned}$$

a pošto je $(n-i)! = \mathrm{V}(n-i, k-i)\cdot(n-k)!$ to je onda

$$\begin{aligned} !n - !(n-k) &= \sum_{i=1}^{k}(n-i)! \\ &= \sum_{i=1}^{n}\mathrm{V}(n-i,k-i)\cdot(n-k)! \\ &= (n-k)!\sum_{i=1}^{k}\mathrm{V}(n-i,k-i) = (n-k)!\,\mathrm{W}(n,k) \end{aligned}$$

Sada izvodimo formulu

$$\begin{aligned} !n &= \sum_{i=0}^{l-1}(!(n-ik) - !(n-(i+1)k) + !(n-lk) \\ &= \sum_{i=0}^{l-1}(!(n-ik) - !(n-ik-k)) + !r \\ &= \sum_{i=0}^{l-1}(n-(i+1)k)!\,\mathrm{W}(n-(i+1)k, n-ik) + !r \end{aligned}$$

Uočimo još da za prirodne brojeve $a, b, A, B \in N$ takve da je $a > b$ važi

$$\begin{aligned} a!\cdot A + b!\cdot B &= b!(a(a-1)\ldots(b+1)\cdot A + B) \\ &= b!(\mathrm{V}(a, a-b) + B) \qquad \text{pa je sada} \\ !n &= (\ldots(\mathrm{W}(n,k)\cdot\mathrm{V}(n-k,k) + \mathrm{W}(n-k,k))\cdot\mathrm{V}(n-2k,k) \\ &\quad + \mathrm{W}(n-2k,k))\cdot\mathrm{V}(n-3k,k) + \cdots + \mathrm{W}(n-(l-1)k,k))\cdot r! + !r \end{aligned}$$

pa sada navedeni niz ima tu osobinu da je $S_l = !n$.

3 Algoritam za proveru Kurepine hipoteze

Proveru Kurepine hipoteze izvodimo koristeći ranije izvedene relacije. Domen na kome vršimo ispitivanje je skup svih prostih brojeva, jer smo dokazali ekvivalentnost

(KH) sa iskazom (E1). Tako, ako (KH) važi za neke proste brojeve p_1, p_2, ... ,p_k onda (KH) važi za sve brojeve oblika $p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$. U računanju levog faktorijela koristimo rekurentnu formulu iz prethodne teoreme za $k = 1$. Pošto je nama potrebna samo informacija o deljivosti broja $!p$ sa p, to je dovoljno sve operacije izvršavati u prstenu $Z = \{0, 1, \ldots, p-1\}$. Na taj način ćemo izbeći problem rada sa velikim brojevima, jer tada možemo izvršavati operacije hardverski implementirane u računaru. Paralelizam možemo ostvariti na više načina. Jedna mogućnost je da sve procesore angažujemo na izračunavanju vrednosti $!n \bmod n$. Tu se pojavljuje problem gubljenja vremena jer sekvencijalan algoritam za izračunavanje niza se ne može idealno paralelizovati. Efikasniji je drugi metod: svakom procesoru dodelimo po jedno n za koje treba ispitati (KH).

Algoritam KH1.

```
{Ulaz :   granice intervala [a,b] u kojem vršimo proveru}
{Izlaz:   informacija o tačnosti (KH)}
{Arhitektura: procesori P0, P1 , ... ,Pk-1 }
01   DO in parallel 0 ≤ i ≤ k − 1
02       P1 :  m = π(a) + 1 + i
03             WHILE pm ≤ b DO
04             s = 1
05             FOR i = pm − 1 DOWNTO 1 DO
06                 s = s ∗ i + 1 mod pm
07             IF s = 0 THEN print:"KONTRAPRIMER"
08             m = m + i
```

Izračunajmo sada $T_1(n)$, vreme potrebno za proveru hipoteze u intervalu $[1..n]$. Pošto se FOR ciklus (05–06) izvršava u vremenu $O(p_m)$, to se primenom Stiltjesovog integrala može dobiti konačna formula:

$$\begin{aligned} T_1(n) &= (1/k)\sum p_i \\ &= (1/k)\int \ln x d\pi(x) \\ &= (1/k)x\pi(x) - (1/k)\int \pi(x)dx(1/k)x\pi(x) \\ &= \frac{x^2}{(k\ln x)} \end{aligned}$$

Dakle $T_1(n) = O(\frac{x^2}{k\,lnx})$ gde je k broj procesora.

4 Realizacija algoritma na računaru

Navedeni algoritam je realizovan na transpjuterskoj ploči sa četiri transpjutera T800. Program je pisan u jeziku 3L Parallel FORTRAN za transpjutere. Posao je

obavljen tako što je prvo napravljena baza prostih brojeva manjih od 1000000, a zatim je svaki procesor ispitivao tačnost iskaza (E1) za odgovarajuću grupu prostih brojeva koja mu je dodeljena. U određenim vremenskim intervalima glavni procesor je skupljao informacije o dobijenim rezultatima svakog procesora. Konačan rezultat nije doneo nikakvu promenu u odnosu na dosadašnje rezultate. Za sve proste brojeve manje od milion iskaz (E1) odnosno (KH) je tačan. Preciznije rečeno, svi prirodni brojevi koji nemaju prost delilac veći od milion zadovoljavaju iskaz Kurepine hipoteze. Ranije provere Kurepine hipoteze su vršili Slavić za $n \leq 1000$, Wagstaff za $n \leq 50000$ i Mijajlović za $n \leq 310009$.

LITERATURA

[1] S. G. Akl, *The design and analysis of parallel algorithms,* Prentice Hall International, 1989.

[2] R. Guy *Unsolved problems in number theory,* Springer–Verlag, 1981.

[3] D. Kurepa, *On some new factorial propositions,* Mathematica Balkanica 4 (1974), 383–386.

[4] Ž. Mijajlović, *On some formulas involving !n and the verification of the !n-hypotesis by use of computers,* Publ. Inst. Math. 47 (1990), 24–32.

[5] D. Kurepa, *On the left factorial function,* Mathematica Balkanica 1 (1971), 147–153.

[6] M. J. Quinn, *Designing efficient algorithms for parallel computers,* McGraw–Hill, 1987.

[7] H. Riesel, *Prime numbers and computer methods for factorization,* Birkhauser, 1985.

Matematički institut
Knez Mihailova 35, P.P. 367
11001 Beograd