BITONIC SORT SARALASH ALGORITMI.

Yusupov Mirsaid Abdulaziz o`g`li

Farg`ona Davlat Unversiteti Amaliy matematika va informatika kafedirasi o`qituvchisi

mirsaidbeky@gmal.com

Ma'rufova Gulsanam Davlatbek qizi

Farg`ona Davlat Unversiteti talabasi

Gulsanammarufova9@gmail.com

Anatatsiya:

Bitonic Sort — bu parallel ishlov berishga mos bo'lgan, taqqoslashga asoslangan saralash algoritmi. U ma'lumotlar ketma-ketligini avval bitonik ketma-ketlikka aylantirib, so'ng uni tartiblash orqali ishlaydi. Algoritm asosan quvvatli parallel protsessorlar uchun samarali hisoblanadi.

Kalit so`z:

Bitonic, Saralash, Parallel algoritm, Taqqoslash, Ketma-ketlik, Yig'ilish, O'suvchi tartib, Kamayuvchi tartib, Rekursiya, Blokli saralash, Parallelizatsiya, Massiv

Аннотация

Bitonic Sort — это алгоритм сортировки, основанный на сравнении и хорошо подходящий для параллельной обработки. Он сначала преобразует последовательность в битоническую, а затем упорядочивает её. Алгоритм эффективен для систем с высокой степенью параллелизма.

Ключевые слова:

Bitonic, Сортировка, Параллельный алгоритм, Сравнение, Последовательность, Объединение, Возрастающий порядок, Убывающий порядок, Рекурсия, Блочная сортировка, Параллелизм, Массив

Annotation

Bitonic Sort is a comparison-based sorting algorithm well-suited for parallel processing. It first transforms a sequence into a bitonic sequence and then sorts it. The algorithm is efficient on systems with high parallelism.

Keywords:

Bitonic, Sorting, Parallel algorithm, Comparison, Sequence, Merging, Ascending order, Descending order, Recursion, Block sorting, Parallelism, Array

Kirish

Zamonaviy hisoblash tizimlarida katta hajmdagi ma’lumotlarni tez va samarali tartiblash muhim masalalardan biridir. Turli sohalarda, jumladan ma’lumotlar bazasi boshqaruvi, kompyuter grafikasi va sun’iy intellektda saralash algoritmlarining roli katta. Bitonic Sort algoritmi — bu parallel ishlov berish imkoniyatlarini to‘liq ishga soluvchi, taqqoslashga asoslangan samarali saralash usulidir. Ushbu algoritm avval ketma-ketlikni maxsus — bitonik ko‘rinishga keltirib, so‘ng uni tartiblash asosida ishlaydi. Bitonic Sort ko‘pincha apparat darajasida (xususan, GPU yoki FPGA) samarali ishlashi bilan ajralib turadi. Shuning uchun u yuqori tezlik va parallel ishlov talab qilinadigan tizimlar uchun qulay yechim hisoblanadi.

Bitonic Sort algoritmi — bu deterministik va parallel ishlovga moslashgan samarali saralash usuli bo‘lib, ayniqsa yuqori samaradorlik talab qilinadigan tizimlarda o‘z o‘rniga ega. Ushbu algoritmning asosiy ustunligi — ma’lumotlar ustida barqaror va oldindan belgilangan tartibda ishlashidir. Bu esa uni nafaqat parallel hisoblash tizimlarida, balki kriptografik muhitlarda, maxfiylikni saqlash talab qilinadigan xavfsiz hisoblash protokollarida ham qo‘llash imkonini beradi.

Bitonic Sort — bu taqqoslashga asoslangan saralash algoritmi bo‘lib, ma’lumotlar ketma-ketligini bitonik ketma-ketlikka aylantirib, so‘ngra uni tartiblash orqali ishlaydi.

Bitonik ketma-ketlik – bu dastlab o‘suvchi, so‘ng kamayuvchi (yoki teskarisi) bo‘lgan sonlar ketma-ketligidir. Misol: 1, 4, 6, 9, 7, 3, 2 — bu bitonik ketma-ketlik.

2. Algoritmning bosqichlari:

1. **Bitonik ketma-ketlik yaratish:**

Kichik guruhlar (bloklar) avval o‘suvchi va kamayuvchi tarzda tartiblanadi.

2. **Bitonic Merge (birlashma) bosqichi:**

Bitonik ketma-ketlikdagi elementlar qiyoslanadi va saralangan holga keltiriladi. Bu bosqich rekursiv tarzda davom etadi.

3. Afzalliklari:

Parallel ishlashga yaroqli: Har bir bosqich mustaqil ishlaydi, bu esa GPU yoki FPGA kabi qurilmalarda tez ishlash imkonini beradi.

Deterministik: Har doim bir xil sonli qadamlar va harakatlar bajariladi.

4. Kamchiliklari:

Faoliyat murakkabligi: Oddiy kompyuterlarda bu algoritm ko‘proq harakat (operatsiya) talab qiladi.

Saralash uchun elementlar soni odatda 2^n bo‘lishi kerak.

5. Amaliy qo‘llanilishi:

Parallel kompyuterlar (xususan, **GPU** hisoblash)

Signalni qayta ishlash

Katta hajmdagi ma’lumotlarni real vaqtda tartiblash

Parallel hisoblash tizimlari (HPC - High Performance Computing):

GPU (grafik protsessor) yoki FPGA (konfiguratsiyalanuvchi integral sxema) asosida ishlaydigan tizimlarda tez va samarali saralash uchun.

Ko‘p yadroli (multi-core) protsessorlarda massivlar bilan bir vaqtda ishlash imkonini beradi.

2. Real vaqtda ishlov berish tizimlari (Real-time Systems):

1) Doimiy ravishda yangi ma’lumotlar kirib keladigan tizimlarda, kechikishni kamaytirish uchun foydalaniladi.

2) Masalan: video oqimlarni qayta ishlash yoki signalni saralashda

3. Raqamli signalni qayta ishlash (DSP - Digital Signal Processing):

1) Tez-tez saralash zarur bo‘lgan filtrlar, spektral tahlil yoki sensorli ma’lumotlar bilan ishlashda.

4. Kompyuter grafikasi

1) GPU'da ishlaydigan shader dasturlarida massivdagi obyektlar yoki piksel qiymatlarini saralashda.

2) Fizik asosli rendering yoki z-buffer saralash jarayonlarida.

5. Telekommunikatsiya va tarmoq uskunalari:

- Paketlarni ustuvorlikka qarab saralash (packet sorting).
- Ma’lumot oqimini boshqarish (traffic shaping).

6. Sun’iy intellekt va mashinaviy o‘rganish

1) Parallel ma’lumot tahlili (feature ranking, preprocessing) bosqichlarida.

2) Katta hajmdagi kirish ma’lumotlarini tez tahlil qilish uchun.

7. Kriptografiya va xavfsizlik:

1) Ba’zi hollarda algoritmlarning deterministik xususiyati kriptografik tizimlar uchun afzal bo‘ladi.

2) Maxfiylikni saqlagan holda saralash algoritmlarida (Secure Sorting).

Kriptografiya va xavfsizlikda Bitonic Sort qo‘llanilishi

1. Secure Sorting (Maxfiylikni saqlagan holda saralash)

Kriptografik tizimlarda ko‘p hollarda saralash kerak bo‘ladi, lekin bu jarayonda **foydalanuvchi ma’lumotlari maxfiy saqlanishi** zarur. Oddiy saralash algoritmlarida:

Har bir element qiymati taqqoslanadi;

Tashqi tomondan kuzatuvchi bu taqqoslashlar asosida ma’lumot strukturasini taxmin qilishi mumkin.

Bitonic Sort esa:

Deterministik – ya’ni har doim bir xil tartibda ishlaydi (qanday ma’lumot bo‘lishidan qat’i nazar).

Shu sababli, **taqqoslashlarning tartibi o‘zgarmaydi**, bu esa **ma’lumot qiymatlari asosida hech qanday yon ma’lumot (side-channel info)** chiqmaydi.

Bu xususiyat **"Oblivious Sorting"** (yashirin saralash) konsepsiyasiga juda mos keladi.

2. Secure Multi-Party Computation (SMPC)

SMPC — bir nechta ishtirokchi o‘zlarining shaxsiy ma’lumotlarini oshkor qilmasdan, birgalikda hisob-kitob bajaradigan kriptografik texnologiya.

Misol: 10 nafar foydalanuvchi o‘z maoshlarini taqqoslashmoqchi, lekin hech kim boshqalarning ma’lumotini bilishni xohlamaydi.

Bunday hollarda:

Bitonic Sort algoritmi **kripto-primitivlar yordamida** (masalan: homomorfik shifrlash, secret sharing) **taqqoslash operatsiyalarini yashirin** bajarishi mumkin.

Har bir bosqichda o‘zgarishlar **kripto-muomala shaklida** bo‘ladi.

3. Side-Channel Attack'lar oldini olish

Oddiy algoritmlar (QuickSort, MergeSort) kirish ma’lumotlariga qarab har xil yo‘nalishda ishlaydi. Bu esa:

Tizimdagi vaqt, xotira yoki energiya o‘zgarishlari orqali **hujumchiga sezilarli signal** berishi mumkin.

Bitonic Sort esa:

Har doim **aniq va oldindan belgilangan yo‘nalishda** ishlaydi;

Shu sababli **side-channel attack’lardan himoyalash** uchun juda mos.

4. Trusted Execution Environment (TEE) ichida ishlash

Kriptografik tizimlar ko‘pincha maxsus muhofaza qilingan muhitda (Intel SGX, ARM TrustZone) bajariladi. Bu muhitlarda:

Har bir ko‘proq nazorat ostida ishlaydi;

Bitonic Sort bu joyda **kutilgan ishlov (deterministik) va parallelizatsiya** sababli resurslardan samarali foydalanadi.

Bitonic Sort algoritmi kriptografik muhitda:

1) **Maxfiylikni saqlash**,
2) **Yon-kanal hujumlaridan himoya qilish**,
3) **Parallel va xavfsiz saralashni amalga oshirish**,
4) **Yashirin taqqoslashlarni kriptografik protokollarga integratsiya qilish** uchun juda foydalidir.

Bu sababli u **oblivious sorting**, **SMPC protokollari**, va **xavfsiz tizim dizayni**da keng qo‘llanilmoqda.

Xulosa

Bitonic Sortning deterministik xususiyati uni **oblivious sorting**, **secure multi-party computation**, va **side-channel attack**’lardan himoyalangan tizimlar uchun muhim vositaga aylantiradi. Shuningdek, u katta hajmdagi massivlar bilan samarali ishlash, real vaqtda saralash va GPU/FPGAlarda optimallashtirilgan amaliyotlar uchun mos keladi. Xulosa qilib aytganda, Bitonic Sort algoritmi nafaqat o‘qitish maqsadida, balki amaliy xavfsiz tizimlar arxitekturasida ham dolzarb ahamiyat kasb etadi.

Foydalanilgan adabiyotlar:

1. Batcher, K. E. (1968). *Sorting networks and their applications*. Proceedings of the AFIPS Spring Joint Computer Conference, 32, 307–314.
2. Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2009). *Introduction to Algorithms* (3rd ed.). MIT Press.
3. Blelloch, G. E. (1990). *Prefix Sums and Their Applications*. Carnegie Mellon University.
4. Knuth, D. E. (1998). *The Art of Computer Programming, Volume 3: Sorting and Searching*. Addison-Wesley.
5. Leighton, F. T. (1992). *Introduction to Parallel Algorithms and Architectures: Arrays, Trees, Hypercubes*. Morgan Kaufmann.
6. Goodrich, M. T. (1999). *Communication-efficient oblivious sorting*. Proceedings of the ACM Symposium on Parallel Algorithms and Architectures.

7. Parhami, B. (2007). *Introduction to Parallel Processing: Algorithms and Architectures*. Springer.

8. Kumar, V., Grama, A., Gupta, A., & Karypis, G. (1994). *Introduction to Parallel Computing*. Benjamin-Cummings.

9. Dolev, S., & Yagel, R. (2009). *Oblivious and efficient sorting and selection*. Journal of Parallel and Distributed Computing.

10. Sedgewick, R., & Wayne, K. (2011). *Algorithms* (4th ed.). Addison-Wesley.

Ilm fan taraqqiyotida raqamli iqtisodiyot va zamonaviy ta'limning o'rni hamda rivojlanish omillari