Список использованных источников

1. Ойнаров Р., Ограниченность и компактность интегральных операторов вольтеровского типа // Сиб. матем. журн. 2007. Т. 48, № 5. С. 1100–1115.
2. Ойнаров Р., Ограниченность и компактность интегральных операторов с переменными пределами интегрирования в весовых пространствах Лебега // Сиб. матем. журн. 2011. Т. 52, № 6. С. 1313–1328.
3. Ойнаров Р. Весовые неравенства для одного класса интегральных операторов // Докл. АН СССР. 1991. Т. 319, №5. С. 1076-1078.
4. Степанов В.Д, Ушакова Е.П., Об интегральных операторах с переменными пределами интегрирования //Труды математического института им. В.А. Стеклова. 2001. Т. 232. С. 298-317 .
5. Батуев Э.Н., Степанов В.Д. Весовые неравенства типа Харди // Препринт /ВЦДВНЦ АН СССР. Владивосток. 1987. 22 с.

УДК 512

АҚПАРАТ ТАСЫМАЛДАУ ХАТТАМАСЫ ЖАЙЛЫ

Дауыл Ұлан
e-mail: akyik.kz.777@mail.ru
Л.Н. Гумилев атындағы Еуразия Ұлттық Университетінің докторанты,
Нұр - Сұлтан, Қазақстан
Ғылыми жетекшісі – Байсалов Е.Р.

Хаттама сипаттамасы.

Хабарласушы жақтар: Алиса (A) және Боб (B).

Платформа: ақырлы өріс үстіндегі $n \times n$ матрицалардың алгебрасы.

Хаттама мақсаты: X матрицасы түрінде кодталған хабарды A-дан B-ға ашық ақпарат арнасы бойынша тасымалдау және сонымен бірге хабардың құпиялылығын қамтамасыз еті.

Хаттама қадамдары:

1. Алиса кездейсоқ керіленетін U матрицасын таңдап, UX-ты есептеп, шыққан нәтиже-матрицаны Бобқа жібереді.
2. Боб кездейсоқ керіленетін V матрицасын таңдап, UXV-ны есептеп, шыққан нәтиже-матрицаны Алисаға жібереді.
3. Алиса алған матрицаны сол жағынан кері U^{-1} матрицасына көбейтіп, шыққан $U^{-1}UXV = XV$ матрицасын Бобқа қайта жібереді.
4. Боб алған матрицаны оң жағынан кері V^{-1} матрицасына көбейтіп, ең соңында $XVV^{-1} = X$ матрицасын алады.

Ескерту. Кейбір авторлар осындай сипаттамадағы хаттамаларда аралық сипатындағы өрескел шабуылдарға тұрақтылықты сақтау мақсатында хаттама элементтеріне түрлі талаптар қояды.

Мысалы, ақырлы өрістің қуаты мен n параметрінің жеткілікті үлкен болу және матрицаның рангы $n/2$ санына жақын және т.с.с.

Сонымен, Оскар атты (O) бақылаушыға қатысты математикалық есептің сипаттамасына көшеміз.

Берілгені: UX, UXV, XV $n \times n$ матрицалары.

Табу керек: X $n \times n$ матрицасы.

Шешуі: Төмендегі алгоритмдік мәселені шешудің тез, жылдам әдісін $C = UX$, $D = UXV$ матрицаларына қолданып, керіленетін W матрицасын анықтаймыз. Сонда

$$XV = U^{-1}UXV = U^{-1}UXW = XW.$$

Демек, енді XV-ны оң жақтан W^{-1} көбейтсек, X-ты аламыз.

Алгоритмдік Есеп. Бізге $n \times n$ D матрицасының $n \times n$ C матрицасының оң жағынан бір керіленетін матрицаға көбейткенде шығатыны белгілі болсын. $D = CW$ болатындай $n \times n$ W матрицасын құрастыруының тиімді алгоритмін табыңыз.

Шешуі: Жалпылықты шектеместен, C матрицасының бірінші r жолдары сызықты тәуелсіз және $r = \mathrm{rank}(C)$ болсын деп ұйғарайық. Осы жолдарды базиске дейін еркін түрде толықтырамыз: бұны матрицаның рангын есептеуде қолданылатын Гаусс әдісімен тиімді түрде жасауға болады. Мысалы, нөлдік емес минор жоғарғы сол бұрышта орналасса, онда бірінші r жолды базиске дейінгі стандартты базистің $e_{r+1}, \ldots, e_n$ векторларымен толықтыруға болады.

Осы базисті C матрицасының бірінші r жолы бар керіленетін $n \times n$ C_0 матрицасын құрастыру үшін қолданайық. D матрицасының бірінші r жолдары сызықты тәуелсіз болады және $r = \mathrm{rank}(D)$. Тағы да жоғарыда айтылған әдісті қайталап бірінші r жолы D матрицасының бірінші r жолына тең болатын, керіленетін $n \times n$ D_0 матрицасын құрастырамыз. $W = C_0^{-1}D_0$ матрицасы есепті шығарады.

Ескерту: Гаусстың элиминация әдісін қолдану үшін C мен D матрицаларын бірінің соңынан бірін жалғап, $n \times 2n$ өлшемді $C\hat{}D$ матрицасын жасауға болады; сонан соң $n \times 2n$ өлшемді $C\hat{}D$ матрицасының ұзындықтары $2n$ жолдарымен жұмыс жасап, элиминация әдісін іске асыра аламыз.

Қолданылған әдебиеттер

1. В.А. Романьков, *Алгебраическая криптография*. Издательство ОГУ им. Ф.М. Достоевского, Омск (2013).

2. Сайт: https://ru.wikipedia.org/wiki/Трёхэтапный_протокол.

УДК 519.651

МАТЕМАТИЧЕСКИЙ АППАРАТ КОМПЬЮТЕРНОЙ (ВЫЧИСЛИТЕЛЬНОЙ) ТОМОГРАФИИ В КОНТЕКСТЕ КОМПЬЮТЕРНОГО (ВЫЧИСЛИТЕЛЬНОГО) ПОПЕРЕЧНИКА