(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0041895
(43) 공개일자 2018년04월25일

(51) 국제특허분류(Int. Cl.)
G06F 17/16 (2006.01)
(52) CPC특허분류
G06F 17/16 (2013.01)
(21) 출원번호 10-2016-0134222
(22) 출원일자 2016년10월17일
심사청구일자 2016년10월17일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
허준
서울특별시 강남구 광평로10길 6, 206동 103호(일원동, 한솔마을아파트)
이신규
서울특별시 동대문구 약령시로 6, 603호 (제기동)
(74) 대리인
특허법인충정

전체 청구항 수 : 총 9 항

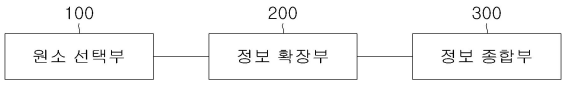
(54) 발명의 명칭 **토플리츠 행렬 처리 장치 및 방법**

(57) 요 약

본 발명은 토플리츠 행렬 처리 장치 및 방법에 관한 것으로, 특히 본 발명은 원소 선택 과정에서 중복 원소를 제거하여 덧셈 연산량을 큰 폭으로 감소시킨 토플리츠 행렬 처리 장치 및 방법에 관한 것이다.

또한, 본 발명에 따르면, 토플리츠 행렬을 소행렬로 분화시키면서 중복 행렬을 제거하고, 2*2 행렬로 분화가 진행되면 이웃하는 소행렬간의 대각선상의 중복 원소를 제거하여 개선된 7차 행렬을 형성하여 곱셈 대상 벡터의 원소를 선택하는 원소 선택부; 상기 원소 선택부에서 선택된 곱셈 대상 벡터의 원소의 수에 대응되도록 정보 벡터의 길이를 확장하는 정보 확장부; 및 상기 정보 확장부의 확장된 정보 벡터와 곱셈 대상 벡터를 곱셈 연산하여 결과를 종합하는 정보 종합부를 포함하여 덧셈 연산량을 감소시킨다.

대 표 도 - 도3



이 발명을 지원한 국가연구개발사업
과제고유번호 1711035212
부처명 미래창조과학부
연구관리전문기관 정보통신기술진흥센터
연구사업명 대학ICT연구센터 육성지원사업
연구과제명 무결점 보안을 위한 지상/위성 양자통신 기술 개발
기 여 율 1/1
주관기관 고려대학교 산학협력단
연구기간 2016.01.01 ~ 2016.12.31

명 세 서

청구범위

청구항 1

토플리츠 행렬을 소행렬로 분화시키면서 중복 행렬을 제거하고, 2*2 행렬로 분화가 진행되면 이웃하는 소행렬간의 대각선상의 중복 원소를 제거하여 개선된 7차 행렬을 형성하여 곱셈 대상 벡터의 원소를 선택하는 원소 선택부;

상기 원소 선택부에서 선택된 곱셈 대상 벡터의 원소의 수에 대응되도록 정보 벡터의 길이를 확장하는 정보 확장부; 및

상기 정보 확장부의 확장된 정보 벡터와 곱셈 대상 벡터를 곱셈 연산하여 결과를 종합하는 정보 종합부를 포함하는 토플리츠 행렬 처리 장치.

청구항 2

청구항 1항에 있어서,

상기 원소 선택부는 개선된 7차 행렬에 복수의 연산자를 사용하여 곱셈 대상 벡터의 원소를 선택하는 토플리츠 행렬 처리 장치.

청구항 3

청구항 1항에 있어서,

상기 원소 선택부는 상기 토플리츠 행렬이 순환 행렬인 경우에 첫번째 행의 마지막 원소를 중복 제거하는 토플리츠 행렬 처리 장치.

청구항 4

청구항 1항에 있어서,

상기 원소 선택부는 원소가 Z0 내지 Z12인 경우에 1차 연산자를 사용하여 Z0는 Z3-Z0로, Z1는 Z4-Z1로, Z2는 Z5-Z2로, Z3는 Z6-Z0로, Z4는 Z7-Z1로, Z5는 Z8-Z2로, Z6은 Z0로, Z7은 Z1로, Z8은 Z2로, 위치 교환과 덧샘을 반복하고, 입력 행렬이 4*4의 행렬이고 원소가 Z0' 내지 Z12'인 경우에 2차 연산자를 사용하여 Z0'는 Z1'-Z0'로, Z1'는 Z2'-Z0'로, Z2'는 Z0'로, Z3'는 Z4'-'Z3로, Z4'는 Z5'-Z3'로, Z5'는 Z3'로, Z6'은 Z7'-Z6'으로, Z7'은 Z8'-Z6'으로, Z8'은 Z6'로, 위치 교환과 덧샘을 반복하여 원소를 선택하는 토플리츠 행렬 처리 장치.

청구항 5

청구항 1항에 있어서,

상기 정보 확장부는 복수의 연산자를 사용하여 선택된 곱셈 대상 벡터의 원소의 수에 대응되도록 정보 벡터의 길이를 확장하는 토플리츠 행렬 처리 장치.

청구항 6

(A) 원소 선택부는 토플리츠 행렬을 소행렬로 분화시키면서 중복 행렬을 제거하는 단계;

(B) 상기 원소 선택부는 2*2 행렬로 분화가 진행되면 이웃하는 소행렬간의 대각선상의 중복 원소를 제거하여 개선된 7차 행렬을 형성하는 단계;

(C) 상기 원소 선택부는 개선된 7차 행렬을 이용하여 곱셈 대상 벡터의 원소를 선택하는 단계;

(D) 정보 확장부는 상기 원소 선택부에서 선택된 곱셈 대상 벡터의 원소의 수에 대응되도록 정보 벡터의 길이를 확장하는 단계; 및

(E) 정보 종합부는 상기 정보 확장부의 확장된 정보 벡터와 곱셈 대상 벡터를 곱셈 연산하여 결과를 종합하는

단계를 포함하는 토플리츠 행렬 처리 방법.

청구항 7

청구항 6항에 있어서,

상기 (C) 단계의 원소 선택부는 개선된 7차 행렬에 복수의 연산자를 사용하여 곱셈 대상 벡터의 원소를 선택하는 토플리츠 행렬 처리 방법.

청구항 8

청구항 6항에 있어서,

상기 (D) 단계 이후에

(F) 상기 원소 선택부는 상기 토플리츠 행렬이 순환 행렬인 경우에 첫번째 행의 마지막 원소를 중복 제거하여 순환 7차 행렬을 형성하는 단계를 더 포함하며,

상기 (C) 단계에서 상기 원소 선택부는 순환 7차 행렬을 이용하여 곱셈 대상 벡터의 원소를 선택하는 토플리츠 행렬 처리 방법.

청구항 9

청구항 6항에 있어서,

상기 (C) 단계의 원소 선택부는 원소가 Z0 내지 Z12인 경우에 1차 연산자를 사용하여 Z0는 Z3-Z0로, Z1는 Z4-Z1로, Z2는 Z5-Z2로, Z3는 Z6-Z0로, Z4는 Z7-Z1로, Z5는 Z8-Z2로, Z6은 Z0로, Z7은 Z1로, Z8은 Z2로, 위치 교환과 덧샘을 반복하고, 입력 행렬이 4*4의 행렬이고 원소가 Z0' 내지 Z12'인 경우에 2차 연산자를 사용하여 Z0'는 Z1'-Z0'로, Z1'는 Z2'-Z0'로, Z2'는 Z0'로, Z3'는 Z4'-'Z3로, Z4'는 Z5'-Z3'로, Z5'는 Z3'로, Z6'은 Z7'-Z6'으로, Z7'은 Z8'-Z6'으로, Z8'은 Z6'로, 위치 교환과 덧샘을 반복하여 원소를 선택하는 토플리츠 행렬 처리 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 토플리츠 행렬 처리 장치 및 방법에 관한 것으로, 특히 본 발명은 원소 선택 과정에서 중복 원소를 제거하여 덧셈 연산량을 큰 폭으로 감소시킨 토플리츠 행렬 처리 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 양자 키 분배 시스템의 비밀성 증폭에서는 토플리츠 행렬-벡터 곱셈 방식의 유니버설 해싱을 통해 정보를 압축하여 도청자에게 노출된 정보를 무의미하게 한다[1].

[0003] 이와 같은 양자 키 분배 시스템의 비밀성 증폭 과정에서 이용되는 토플리츠 행렬은 도 1과 같은 구조를 가지고 있다.

[0004] 토플리츠 행렬은 첫 행과 열만으로 행렬 전체를 나타낼 수 있어 자원적인 면에서 경제적이고, 적은 수의 원소로 행렬 연산을 수행할 수 있어서 연산 복잡도 측면에서 효율적이다.

[0005] 비밀성 증폭에서 사용되는 해시 함수는 유니버설 해시함수를 사용해야 한다[1]. 토플리츠 행렬-벡터 곱셈 방식은 유니버설 함수에 해당하기 때문에 현재 존재하는 양자 키 분배 시스템에서 가장 많이 사용되는 기법이다[2].

[0006] 토플리츠 행렬-벡터 곱셈을 위한 알고리즘 중 하나인 7차(7-Order) 알고리즘은 도 2의 순서로 진행된다.

[0007] 도 2a를 참조하면, 7자 모양으로 행렬을 나누어 선택된 원소를 제외한 정보는 사용하지 않는다. 대각선상에 위치한 원소들이 모두 동일한 성질 때문에 중복 원소를 생략하여 연산을 진행하는 것이 7차(7-Order) 알고리즘의 핵심이라고 할 수 있다.

[0008] 선택된 원소를 도 2b를 참조하면, 왼쪽 그림의 입력으로 사용한다. 그래프를 따라서 연산을 진행 후 얻어진 벡터 S는 도 2b를 참조하면 오른쪽 그림의 중앙에 위치한 원에 일렬로 나열된다.

[0009] 이것이 원소가 선택되는 과정이다. 곱해질 정보 벡터 X의 네 개의 원소가 각각 알고리즘을 따라 위치 교환과 덧

셈을 반복하여 벡터 S의 수와 같아지면 S와 X를 곱한다. X를 확장하여 S와 곱하는 과정을 정보 벡터를 확장하는 과정이라고 할 수 있다. 마지막으로, 확장시킨 정보를 종합하여 원하는 결과를 얻어낸다.

[0010] 이와 같은 종래 기술에 따른 7차(7-Order) 알고리즘은 토플리츠 행렬의 특징을 이용하여 같은 원소들을 묶어서 연산하는 것으로 덧셈 연산과 곱셈 연산의 감소가 가능했다.

[0011] 그러나, 7차(7-Order) 알고리즘은 여전히 많은 수의 덧셈 연산량을 필요로 하는 단점이 존재한다.

선행기술문헌

비특허문헌

[0012] (비특허문헌 0001) [1] C. H. Bennet, G. Brassard, C. Crepeau, and U. M. Maurer, Senior Member, IEEE "Generalized Privacy Amplification", TRANSACTIONS OF INFORMATION THEORY, vol. 41, no. 6, pp. 1915-1923, 1995.

(비특허문헌 0002) [2] H. Krawczyk, "LFSR-based Hashing and Authentication", Cryptology-CRYPTO'94, pp. 129-139, 1994.

(비특허문헌 0003) [3] A. Cariow, M. GLISZCZYNSKI, "Fast algorithms to compute matrix-vector products for Toeplitz and Hankel matrices", 2012.

발명의 내용

해결하려는 과제

[0013] 본 발명은 상기와 같은 문제점을 해결하기 위한 것으로, 원소 선택 과정에서 중복 원소를 제거하여 덧셈 연산량을 큰 폭으로 감소시킨 토플리츠 행렬 처리 장치 및 방법을 제공하는 데 있다.

과제의 해결 수단

[0014] 본 발명의 일 측면은 토플리츠 행렬을 소행렬로 분화시키면서 중복 행렬을 제거하고, 2*2 행렬로 분화가 진행되면 이웃하는 소행렬간의 대각선상의 중복 원소를 제거하여 개선된 7차 행렬을 형성하여 곱셈 대상 벡터의 원소를 선택하는 원소 선택부; 상기 원소 선택부에서 선택된 곱셈 대상 벡터의 원소의 수에 대응되도록 정보 벡터의 길이를 확장하는 정보 확장부; 및 상기 정보 확장부의 확장된 정보 벡터와 곱셈 대상 벡터를 곱셈 연산하여 결과를 종합하는 정보 종합부를 포함한다.

[0015] 또한, 본 발명의 일 측면의 상기 원소 선택부는 개선된 7차 행렬에 복수의 연산자를 사용하여 곱셈 대상 벡터의 원소를 선택한다.

[0016] 또한, 본 발명의 일 측면의 상기 원소 선택부는 상기 토플리츠 행렬이 순환 행렬인 경우에 첫번째 행의 마지막 원소를 중복 제거한다.

[0017] 또한, 본 발명의 일 측면의 상기 원소 선택부는 원소가 Z0 내지 Z12인 경우에 1차 연산자를 사용하여 Z0는 Z3-Z0로, Z1는 Z4-Z1로, Z2는 Z5-Z2로, Z3는 Z6-Z0로, Z4는 Z7-Z1로, Z5는 Z8-Z2로, Z6은 Z0로, Z7은 Z1로, Z8은 Z2로, 위치 교환과 덧샘을 반복하고, 입력 행렬이 4*4의 행렬이고 원소가 Z0' 내지 Z12'인 경우에 2차 연산자를 사용하여 Z0'는 Z1'-Z0'로, Z1'는 Z2'-Z0'로, Z2'는 Z0'로, Z3'는 Z4'-'Z3로, Z4'는 Z5'-Z3'로, Z5'는 Z3'로, Z6'은 Z7'-Z6'으로, Z7'은 Z8'-Z6'으로, Z8'은 Z6'로, 위치 교환과 덧샘을 반복하여 원소를 선택한다.

[0018] 또한, 본 발명의 일 측면의 상기 정보 확장부는 복수의 연산자를 사용하여 선택된 곱셈 대상 벡터의 원소의 수에 대응되도록 정보 벡터의 길이를 확장한다.

[0019] 한편, 본 발명의 다른 측면은 (A) 원소 선택부는 토플리츠 행렬을 소행렬로 분화시키면서 중복 행렬을 제거하는 단계; (B) 상기 원소 선택부는 2*2 행렬로 분화가 진행되면 이웃하는 소행렬간의 대각선상의 중복 원소를 제거하여 개선된 7차 행렬을 형성하는 단계; (C) 상기 원소 선택부는 개선된 7차 행렬을 이용하여 곱셈 대상 벡터의 원소를 선택하는 단계; (D) 정보 확장부는 상기 원소 선택부에서 선택된 곱셈 대상 벡터의 원소의 수에 대응되도록 정보 벡터의 길이를 확장하는 단계; 및 (E) 정보 종합부는 상기 정보 확장부의 확장된 정보 벡터와 곱셈

대상 벡터를 곱셈 연산하여 결과를 종합하는 단계를 포함한다.

[0020] 또한, 본 발명의 다른 측면의 상기 (C) 단계의 원소 선택부는 개선된 7차 행렬에 복수의 연산자를 사용하여 곱셈 대상 벡터의 원소를 선택한다.

[0021] 또한, 본 발명의 다른 측면의 상기 (D) 단계 이후에 (F) 상기 원소 선택부는 상기 토플리츠 행렬이 순환 행렬인 경우에 첫번째 행의 마지막 원소를 중복 제거하여 순환 7차 행렬을 형성하는 단계를 더 포함하며, 상기 (C) 단계에서 상기 원소 선택부는 순환 7차 행렬을 이용하여 곱셈 대상 벡터의 원소를 선택한다.

[0022] 또한, 본 발명의 다른 측면의 상기 (C) 단계의 원소 선택부는 원소가 Z0 내지 Z12인 경우에 1차 연산자를 사용하여 Z0는 Z3-Z0로, Z1는 Z4-Z1로, Z2는 Z5-Z2로, Z3는 Z6-Z0로, Z4는 Z7-Z1로, Z5는 Z8-Z2로, Z6은 Z0로, Z7은 Z1로, Z8은 Z2로, 위치 교환과 덧샘을 반복하고, 입력 행렬이 4*4의 행렬이고 원소가 Z0' 내지 Z12'인 경우에 2차 연산자를 사용하여 Z0'는 Z1'-Z0'로, Z1'는 Z2'-Z0'로, Z2'는 Z0'로, Z3'는 Z4'-'Z3로, Z4'는 Z5'-Z3'로, Z5'는 Z3'로, Z6'은 Z7'-Z6'으로, Z7'은 Z8'-Z6'으로, Z8'은 Z6'로, 위치 교환과 덧샘을 반복하여 원소를 선택한다.

발명의 효과

[0023] 본 발명에 따르면, 7차(7-Order) 알고리즘의 전체 덧셈 연산량 중 50~70%의 비중을 차지하는 원소 선택의 과정을 개선하여 연산 복잡도를 감소시킨다.

[0024] 또한, 본 발명에 따르면, 토플리츠 행렬의 특징을 이용하여 원소 선택에서 더 많은 중복 정보를 생략하는 것으로 연산 복잡도를 감소시킨다.

도면의 간단한 설명

[0025] 도 1은 토플리츠 행렬을 보여주는 도면이다.

도 2a는 토플리츠 행렬-벡터 곱셈을 위해 선택된 행렬을 보여주며, 도 2b는 7차(7-Order) 알고리즘을 보여준다.

도 3은 본 발명의 일 실시예에 따른 토플리츠 행렬 처리 장치의 구성도이다.

도 4는 본 발명의 일 실시예에 따른 토플리츠 행렬 처리 방법의 흐름도이다.

도 5a 내지 5d는 개선된 7차 행렬의 원소 선택 과정을 보여주는 일예이다.

도 6은 순환 행렬을 보여주는 예시도이다.

도 7a와 7b는 순환 7차 행렬의 원소 선택 과정을 보여주는 도면이다.

도 8a는 토플리츠 행렬을 보여주는 도면이고, 도 8b는 1차 연산자를 사용하는 결과를 보여주며, 도 8c는 2차 연산자를 사용하는 결과를 보여주며, 도 8d는 1차 연산자 및 2차 연산자를 보여주는 도면이다.

도 9a는 개선된 7차 행렬에 1차 연산자를 사용하는 결과를 보여주는 도면이고, 도 9b는 개선된 7차 행렬에 2차 연산자를 사용하는 결과를 보여주는 도면이다.

도 10a는 순환 7차 행렬에 1차 연산자를 사용하는 결과를 보여주는 도면이고, 도 10b는 순환 7차 행렬에 2차 연산자를 사용하는 결과를 보여주는 도면이다.

도 11a은 정보 벡터 확장 과정을 보여주고 있으며, 도 11b는 종합 과정을 보여주는 예시도이다.

도 12a는 종래 기술의 연산량을 보여주며, 도 12b는 본 발명의 연산량을 보여주는 예시도이다.

도 13은 개선된 7차 행렬을 사용한 경우의 연산량을 보여주는 비교도이다.

도 14는 순환 7차 행렬을 사용한 경우의 연산량을 보여주는 비교도이다.

발명을 실시하기 위한 구체적인 내용

[0026] 본 발명과 본 발명의 동작상의 이점 및 본 발명의 실시에 의하여 달성되는 목적을 설명하기 위하여 이하에서는 본 발명의 바람직한 실시예를 예시하고 이를 참조하여 살펴본다.

[0027] 먼저, 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니며, 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함할 수 있다. 또한

본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서 상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0028] 본 발명을 설명함에 있어서, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다.

[0029] 도 3은 본 발명의 일 실시예에 따른 토플리츠 행렬 처리 장치의 구성도이고 , 도 4는 본 발명의 일 실시예에 따른 토플리츠 행렬 처리 방법의 흐름도이다.

[0030] 도 3을 참조하면, 본 발명의 일 실시예에 따른 토플리츠 행렬 처리 장치는 원소 선택부(100), 정보 확장부(200) 및 정보 종합부(300)로 이루어져 있다.

[0031] 상기 원소 선택부(100)는 2^m*2^m(m은 자연수)의 크기의 토플리츠 행렬을 2로 나눈 크기의 토플리츠 소행렬로 분화시킨 후에 중복 행렬 부분을 제거한다.

[0032] 상기 원소 선택부(100)는 이러한 과정을 반복하여 2*2의 크기의 토플리츠 소행렬로 분화시킨 후에 대각선상의 중복 원소를 제거한 후에, 이웃하는 소행렬간 대각선상의 중복 원소를 제거한다(S100).

[0033] 이를 도 5를 참조하여 설명하면, 도 5a를 참조하면, 8*8 크기의 토플리츠 행렬을 보여주는데, 이를 4*4 크기의 토플리츠 소행렬로 분화시킨 후에 1 내지 3번의 소행렬은 남겨두고 1번 소행렬과 중복되는 1-1번 소행렬을 제거한다.

[0034] 그리고, 도 5b를 참조하면, 4*4 크기의 토플리츠 소행렬을 2*2 크기의 소행렬로 분화시킨 후에, 1번과 같은 1-1의 소행렬을 제거하고, 4와 같은 4-1의 소행렬을 제거하며, 7과 같은 7-1의 소행렬을 제거한다.

[0035] 이후에, 도 5c를 참조하면, 2*2 크기의 소행렬에서 대각선상의 중복 원소를 제거하는데, 1과 같은 1-1 원소와, 4와 같은 4-1 원소, 7과 같은 7-1 원소, 10과 같은 10-1 원소, 13과 같은 13-1 원소, 16과 같은 16-1 원소, 19와 같은 19-1 원소, 22와 같은 22-1 원소 그리고 25와 같은 25-1 원소를 제거한다.

[0036] 이후에, 도 5d를 참조하면, 이웃하는 소행렬간의 대각선상의 중복되는 원소를 제거하게 되는데, 2와 같은 6 원소, 3과 같은 8원소, 11과 같은 15 원소,21과 같은 26원소, 22와 같은 24 원소를 제거한다.

[0037] 이와 같은 과정을 거쳐 원소 선택부(100)는 첫행과 첫열에 해당하지 않은 원소를 제거한 개선된 7자 모양의 4*4 크기의 소행렬을 구한다.

[0038] 그 결과, 종래 기술의 7차 알고리즘에 사용되는 도 5c의 행렬은 27개 원소가 항상 연산에 참여하지만, 본 발명에 사용되는 도 5d의 행렬은 21개 원소만 연산에 참여하여 큰 폭으로 덧셈 연산량을 감소시킬 수 있다.

[0039] 한편, 토플리츠 행렬의 특수한 경우에 해당하는 행렬로 순환행렬(Cirulant matrix)이 있다.

[0040] 순환 행렬은 도 6에 도시된 바와 같으며, 대각 성분이 모두 일치하기 때문에 토플리츠 행렬이다.

[0041] 이와 같은 순환 행렬은 원소들이 한 칸씩 이동하기에 같은 원소들이 순환적으로 나타난다. 그 결과, 중복되는 정보가 일반적인 토플리츠 행렬에 비해 더 많기 때문에 선택할 원소를 더 줄이는 것이 가능하다.

[0042] 따라서, 원소 선택부(100)는 2^m*2^m(m은 자연수)의 크기의 순환 행렬을 2로 나눈 크기의 순환 소행렬로 분화시킨 후에 중복 행렬 부분을 제거할 때에, 순환 행렬은 일반적인 토플리츠 행렬보다 더 많은 부분이 제거된다.

[0043] 그리고, 상기 원소 선택부(100)가 이러한 과정을 반복하여 2*2의 크기의 순환 소행렬로 분화시킨 후에 대각선상의 중복 원소를 제거한 후에, 이웃하는 소행렬간 대각선상의 중복 원소를 제거하며 그에 더해 첫번째 열의 마지막에 존재하는 원소도 제거한다(S100).

[0044] 이를 도 7을 참조하여 설명하면, 도 7a를 참조하면, 4*4 크기의 순환 행렬을 보여주는데, 이를 2*2 크기의 순환 소행렬로 분화시킨 후에 1과 2번의 소행렬은 남겨두고 1번 소행렬과 중복되는 1-1번 소행렬과, 2번 소행렬과 중복되는 2-1의 소행렬을 제거한다.

[0045] 그리고, 도 7b를 참조하면, 이웃하는 소행렬간의 대각선상의 중복되는 원소를 제거하게 되는데, 2와 같은 6 원소를 제거하며, 그에 더해 첫번째 행의 마지막 열에 있는 5번 원소를 제거한다.

[0046] 이와 같은 과정을 거쳐 원소 선택부(100)는 첫행과 첫열에 해당하지 않은 원소를 제거하고, 첫행의 마지막 열을 제거한 개선된 7자 모양의 4*4크기의 소행렬을 구한다.

[0047] 또한, 원소 선택부(100)는 개선된 7자 모양의 4*4 크기의 소행렬을 1차 연산자와 2차 연산자를 사용하여 곱셈 대상 벡터 S를 생성한다.

[0048] 이를 좀더 상세하게 살펴보면, 원소 선택부(100)는 도 8을 참조하면, 도 8a의 4*4의 행렬에 대하여 도 8b의 점선은 음수이고 실선은 양수인 1차 연산자를 사용하여 Z0는 Z3-Z0로, Z1는 Z4-Z1로, Z2는 Z5-Z2로, Z3는 Z6-Z0로, Z4는 Z7-Z1로, Z5는 Z8-Z2로, Z6은 Z0로, Z7은 Z1로, Z8은 Z2로, 위치 교환과 덧샘을 반복한다.

[0049] 이후에, 도 8c에 도시된 바와 같이 도 8b의 결과물에 대하여 음수이고 실선은 양수인 2차 연산자를 사용하여 Z0'는 Z1'-Z0'로, Z1'는 Z2'-Z0'로, Z2'는 Z0'로, Z3'는 Z4'-Z3'로, Z4'는 Z5'-Z3'로, Z5'는 Z3'로, Z6'은 Z7'-Z6'으로, Z7'은 Z8'-Z6'으로, Z8'은 Z6'로, 위치 교환과 덧샘을 반복한다. 이러한 2차례 연산을 표현한 것이 도 8d이다.

[0050] 이때, 본 발명의 원소 선택부(100)는 토플리츠 행렬에서 중복되는 부분을 제거하기 때문에 Z5와 Z7이 생략되어 도 8b는 도 9a와 같이 된다. 물론 도 8c는 도 9b와 같이 변화가 없다.

[0051] 물론, 본 발명의 원소 선택부(100)는 순환 행렬의 경우에는 중복되는 부분이 더 제거되기 때문에 Z4,Z5,Z6,Z7,Z8이 생략되어 도 8b는 도 10a와 같이 된다. 도 8c는 도 10b와 같이 변화가 없다.

[0052] 그리고, 정보 확장부(200)는 중앙에 위에서 구한 결과 벡터 S를 놓고 곱해질 정보 벡터 X를 알고리즘에 따라 위치 교환과 덧샘을 반복하여 벡터 S의 수와 같아지도록 정보 벡터 X를 확장한다(S200).

[0053] 이는 도 11a와 도 11b를 보면, 정보 확장부(200)는 1차 연산자를 사용하여 4개의 정보 벡터 요소를 6개로 확장한 후에 2차 연산자를 사용하여 9개의 원소를 갖는 확장된 정보 벡터 X를 얻는다.

[0054] 즉, 1차 연산자를 사용하여 x_0,x_1,x_2,x_3를, x_2,x_3,x_0,x_1,x_0+x_2, x_1+x_3로 확장하고, 2차 연산자를 사용하여, x_3,x_2,x_2+x_3, x_1, x_0, x_0+x_1, x_1+x_3, x_0+x_2, $x_0+x_1+x_2+x_3$로 확장한다.

[0055] 다음에, 정보 종합부(300)는 곱셉 대상 벡터 S에 확장된 정보 벡터 X를 곱하여 원하는 결과를 산출한다(S300).

[0056] 이는 출력을 y_0는 $s_0'+s_2'+s_6'+s_8'$이며, y_1은 $s_1'+s_7'+s_8'$이며, y_2는 $s_3'+s_5'+s_6'+s_8'$이며, y_3는 $s_4'+s_7'+s_8'$이다.

[0057] 여기에서, s_0', s_1', s_2', s_3', s_4', s_5', s_6', s_7', s_8'은 확장된 정보 벡터의 해당 요소와 곱셉 대상 벡터 S의 곱셈 결과값을 나타낸다.

[0058] 도 12의 노드를 따라 연산량을 비교하면 감소를 확인할 수 있다. 즉, 도 12a는 기존의 연산량으로 처음에 18회의 덧샘량이 필요하지만, 도 12b는 개선된 방법으로 14회가 필요하여 연산량이 줄어들었다.

[0059] 기존의 7-Order 알고리즘과 개선된 7-Order 알고리즘의 원소 선택에 요구되는 연산량의 일반화된 식과 연산 복잡도는 표 1과 같다. 토플리츠 행렬은 n*n($n=2^m$이며, m은 자연수임)

[0060] (표 1)

[0061]

	기존 7-Order 원소 선택	개선된 7-Order 원소 선택
덧셈 연산량	$m \times (2 \times 3^{m-1})$	$\sum_{i=0}^{m-1} (2^{m-i}-1) \times 2 \times 3^i$
O notation	$O(n^{\log 3} \times \log n)$	$O(n^{\log 3})$

[0062] Big O notation을 이용하여 연산 복잡도를 비교하였다. 연산량의 비교는 다음 표 2와 같으며, 도 13과 같다. 곱셈 연산량에 비하여 덧셈 연산량이 월등히 많기 때문에 덧셈 연산량 감소의 효과는 의미있는 결과라 할 수 있다.

[0063] (표 2)

m	7-order	Improved 7-order	Multiplication
1	5	5	3
2	27	27	9
3	111	107	27
4	411	375	81
5	1,443	1,235	243
6	4,911	4,007	729
7	16,383	12,099	2,187
8	53,907	37,191	6,561
9	175,611	113,363	19,683
10	567,735	343,671	59,049
11	1,824,375	1,038,179	177,147
12	5,833,563	3,128,871	531,441

[0064]

[0065] 기존의 7-Order 알고리즘과 순환 7order 알고리즘의 원소 선택에 요구되는 연산량의 비교는 표3과 같으며, 도 14와 같다. 순환 행렬은 n*n($n=2^m$이며, m은 자연수임)이다.

[0066] (표 3)

m	7-order	순환 행렬 7-Order
1	5	4
2	27	20
3	111	78
4	411	278
5	1,443	932
6	4,911	3,004
7	16,383	9,522
8	53,907	29,154
9	175,611	88,944
10	567,735	270,101
11	1,824,375	817,166
12	5,833,563	2,465,518

[0067]

[0068] 본 발명에서는 7-Order 알고리즘에서 중복되는 원소를 통한 연산을 생략하여 연산량을 감소시키는 것으로 연산 복잡도를 감소시킬 수 있음을 확인하였다.

[0069] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서 본 발명에 기재된 실시예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 발명의 기술 사상이 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의해서 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

부호의 설명

[0070] 100 : 원소 선택부 200 : 정보 확장부

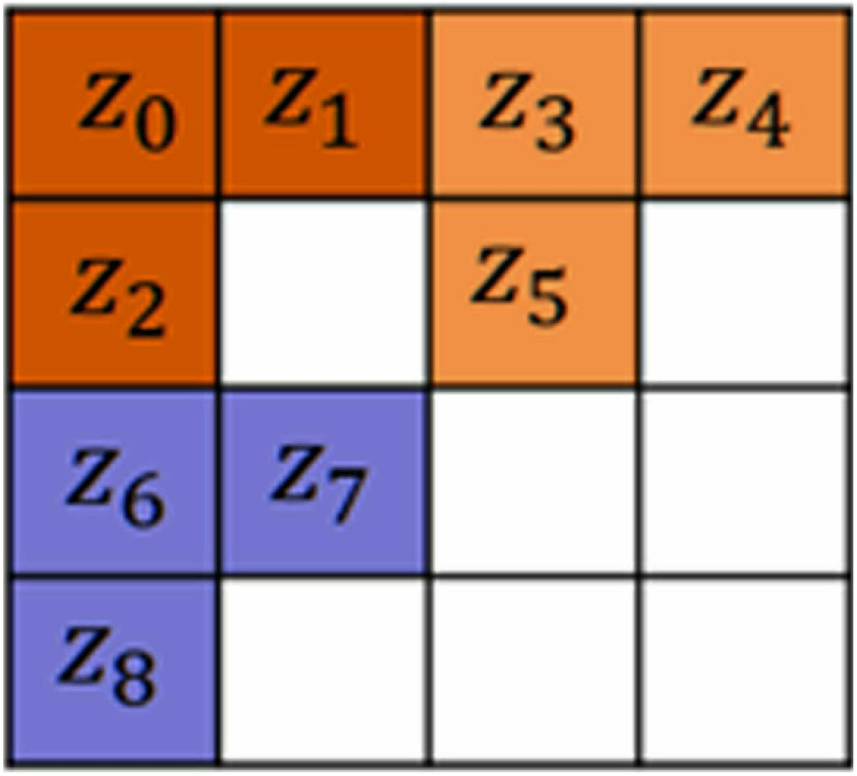
300 : 정보 종합부

도면

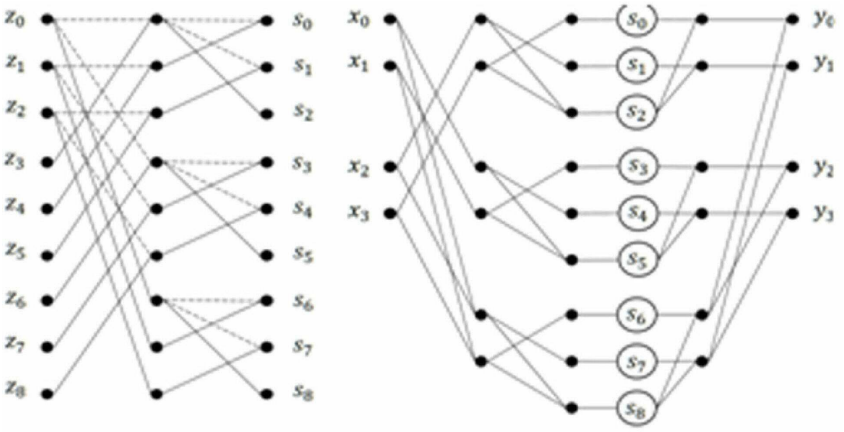
도면1

$$T=\begin{bmatrix} a_0 & a_{-1} & a_{-2} & \cdots & \cdots & a_{-n+1} \\ a_1 & a_0 & a_{-1} & \ddots & & \vdots \\ a_2 & a_1 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & a_{-1} & a_{-2} \\ \vdots & & \ddots & a_1 & a_0 & a_{-1} \\ a_{n-1} & \cdots & \cdots & a_2 & a_1 & a_0 \end{bmatrix}$$

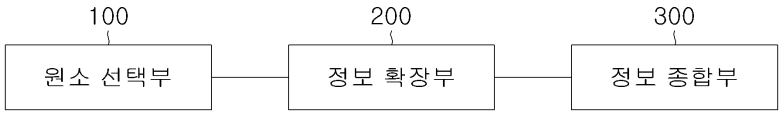
도면2a



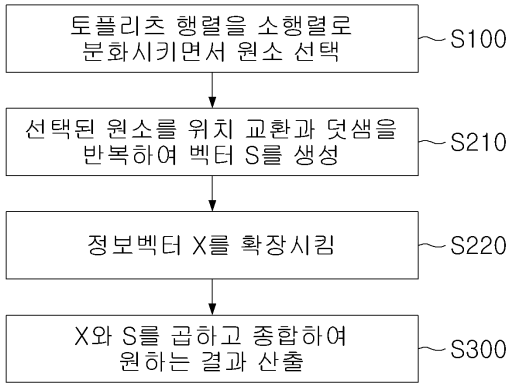
도면2b



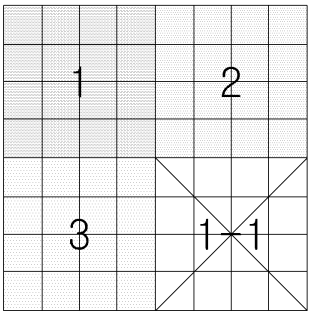
도면3



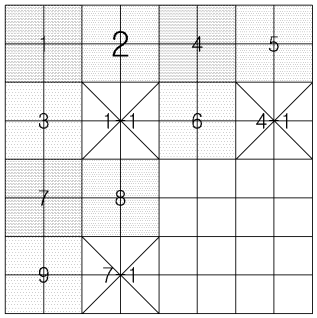
도면4



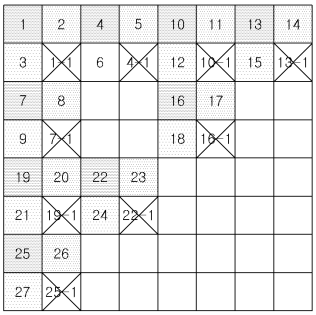
도면5a



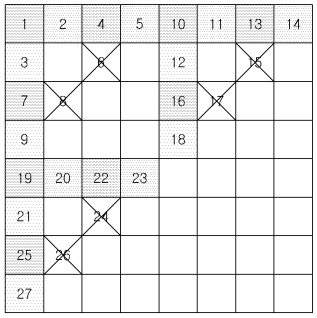
도면5b



도면5c



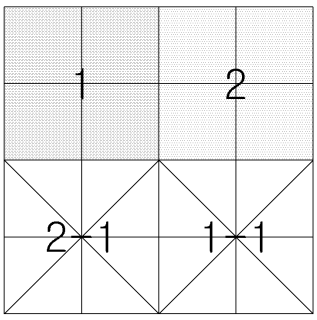
도면5d



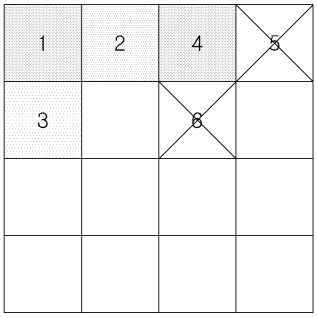
도면6

$$C = \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & \cdots & a_k \\ a_k & \ddots & & & & a_{k-1} \\ a_{k-1} & & \ddots & & & \vdots \\ \vdots & & & \ddots & & \vdots \\ \vdots & & & & \ddots & a_1 \\ a_1 & a_2 & \cdots & \cdots & a_k & a_0 \end{bmatrix}$$

도면7a



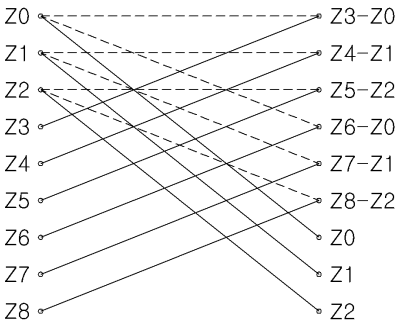
도면7b



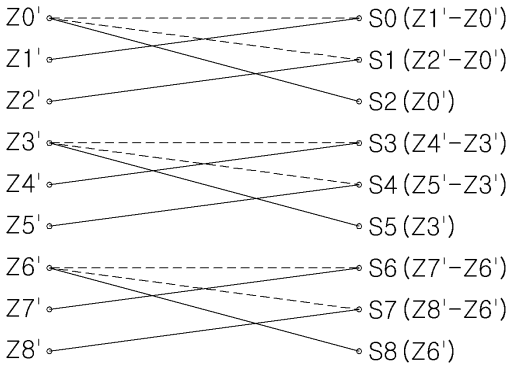
도면8a

Z0	Z1	Z2	Z3
Z4		Z5	
Z6	Z7		
Z8			

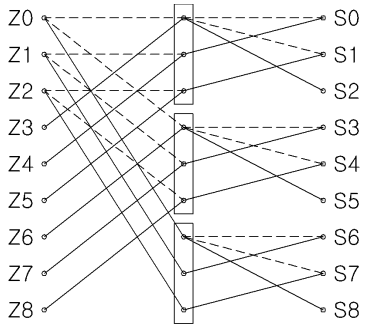
도면8b



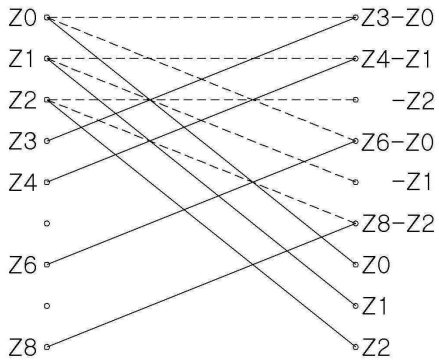
도면8c



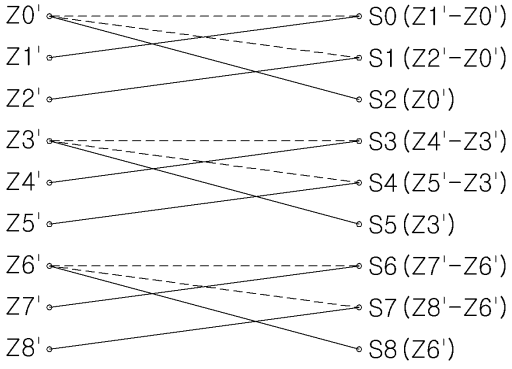
도면8d



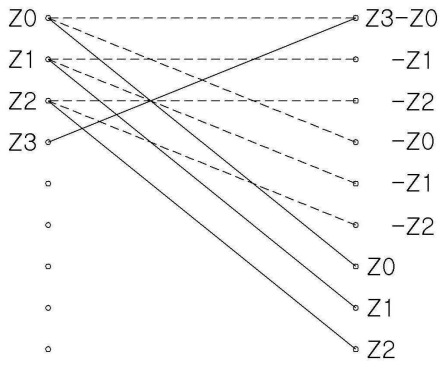
도면9a



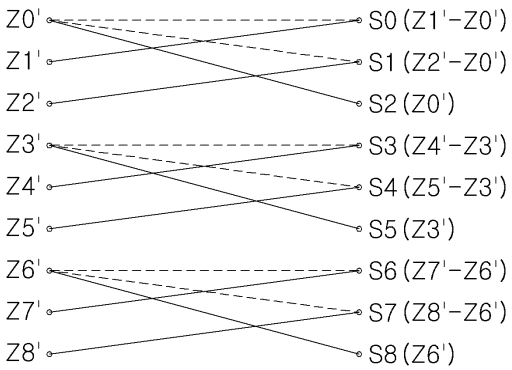
도면9b



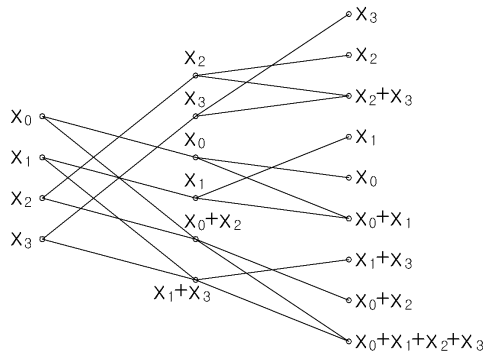
도면10a



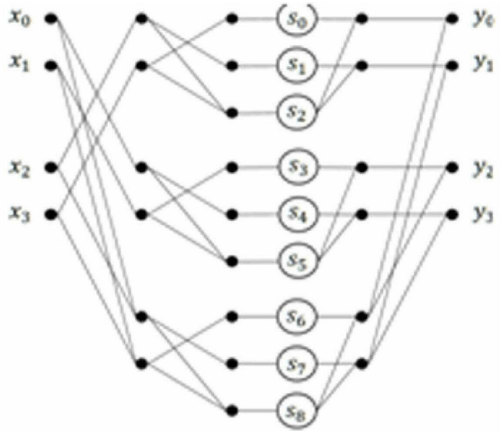
도면10b



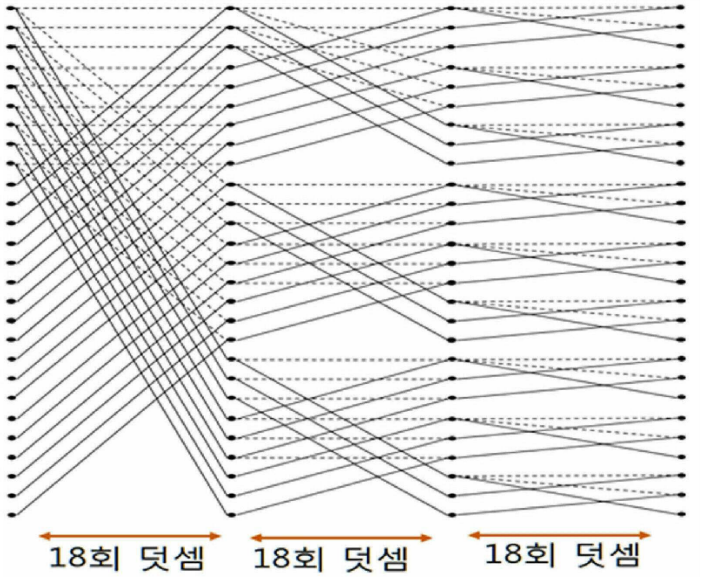
도면11a



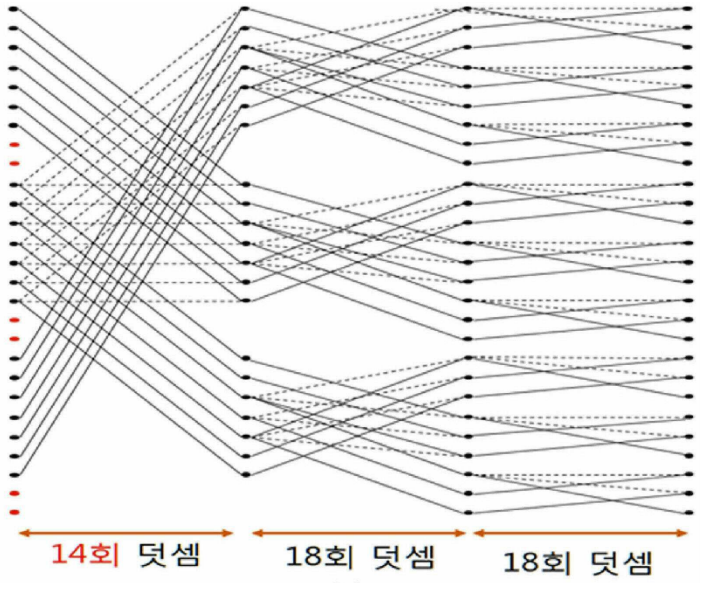
도면11b



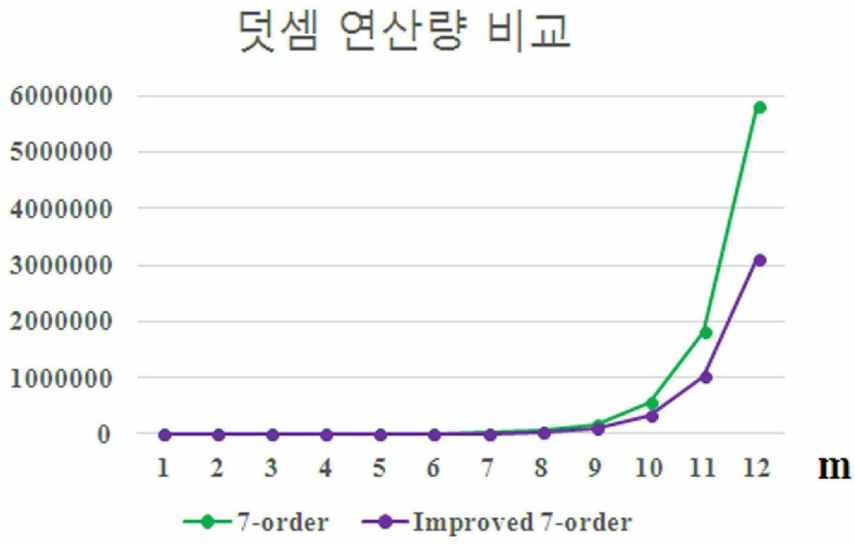
도면12a



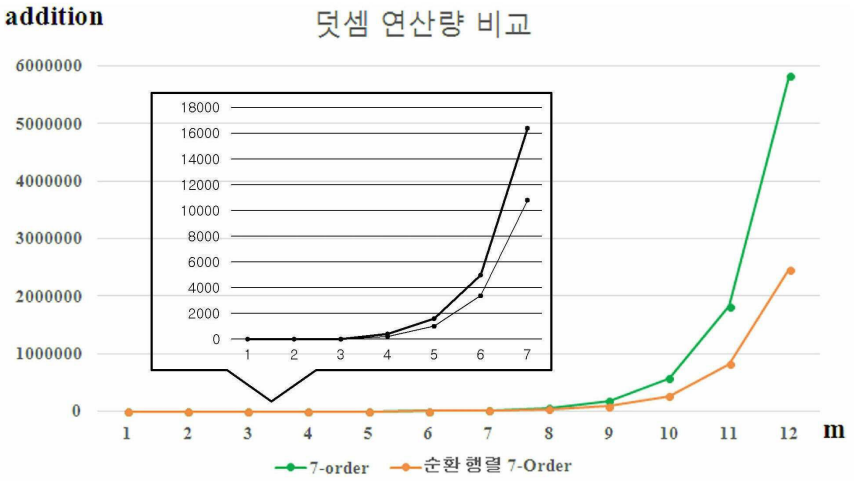
도면12b



도면13


덧셈 연산량 비교
6000000
5000000
4000000
3000000
2000000
1000000
0
1 2 3 4 5 6 7 8 9 10 11 12
m
7-order
Improved 7-order

도면14


addition
덧셈 연산량 비교
6000000
5000000
4000000
3000000
2000000
1000000
0
18000
16000
14000
12000
10000
8000
6000
4000
2000
0
1 2 3 4 5 6 7
1 2 3 4 5 6 7 8 9 10 11 12
m
7-order
순환 행렬 7-Order