



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0130982
(43) 공개일자 2021년11월02일

(51) 국제특허분류(Int. Cl.)
G06Q 50/26 (2012.01) G06F 17/10 (2006.01)
G06F 21/60 (2013.01)
(52) CPC특허분류
G06Q 50/26 (2013.01)
G06F 17/10 (2013.01)
(21) 출원번호 10-2020-0049192
(22) 출원일자 2020년04월23일
심사청구일자 없음

(71) 출원인
한국전력공사
전라남도 나주시 전력로 55(빛가람동)
덕성여자대학교 산학협력단
서울특별시 도봉구 삼양로144길 33 (쌍문동)
경희대학교 산학협력단
경기도 용인시 기흥구 덕영대로 1732 (서천동, 경
희대학교 국제캠퍼스내)
(72) 발명자
이상준
서울시 성북구 길음로 114, 414동 401호
박태정
경기도 고양시 일산동구 위시티1로 7(식사동, 위
시티블루밍5단지아파트) 302-1701
송현주
서울시 성북구 돌곶이로 8길 22, 107동 901호
(74) 대리인
특허법인아주

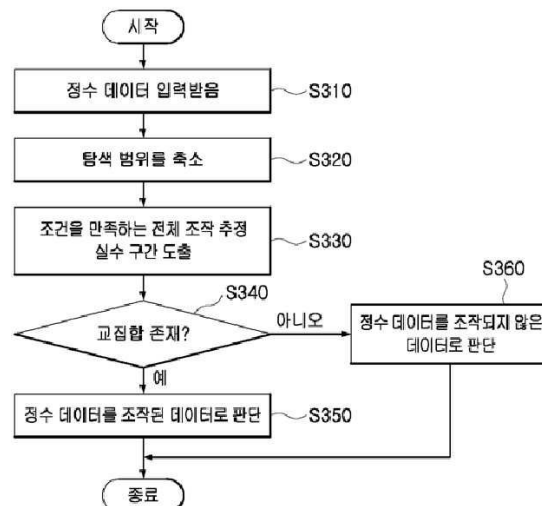
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 데이터 조작 감지 방법 및 장치

(57) 요약

데이터 조작 감지 방법 및 장치가 개시된다. 본 발명의 일 측면에 따른 데이터 조작 감지 방법은, 제어부가 정수로 구성된 정수 데이터에 대해, 각 정수 데이터 간의 차를 활용하여 탐색 범위를 축소하는 단계, 상기 제어부가 상기 축소된 탐색 범위에서 조작에 사용된 것으로 추정되는 조작 추정 실수의 구간을 도출하는 단계, 및 상기 제어부가 상기 도출된 조작 추정 실수의 구간에 기초하여 상기 정수 데이터의 조작 여부를 판단하는 단계를 포함한다.

대표도 - 도3



(52) CPC특허분류

G06F 21/60 (2013.01)

G06Q 2230/00 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	R18XA01
과제번호	R18XA01
부처명	한국전력공사
과제관리(전문)기관명	전력연구원(KEPCO)
연구사업명	전력산업 기초연구 에너지 거점대학 클러스터
연구과제명	알파그리드 플랫폼 설계 및 요소기술 연구
기 여 율	1/1
과제수행기관명	명지대학교 산학협력단 (참여대학 : 덕성여자대학교 산학협력단)
연구기간	2018.03.01 ~ 2021.02.28

명세서

청구범위

청구항 1

제어부가 정수로 구성된 정수 데이터에 대해, 각 정수 데이터 간의 차를 활용하여 탐색 범위를 축소하는 단계;
 상기 제어부가 상기 축소된 탐색 범위에서 조작에 사용된 것으로 추정되는 조작 추정 실수의 구간을 도출하는 단계; 및
 상기 제어부가 상기 도출된 조작 추정 실수의 구간에 기초하여 상기 정수 데이터의 조작 여부를 판단하는 단계를 포함하는 데이터 조작 감지 방법.

청구항 2

제1항에 있어서,
 상기 탐색 범위를 축소하는 단계에서,
 상기 제어부는, $2 \log \Delta y$ 로 탐색 범위를 축소하는 것을 특징으로 하는 데이터 조작 감지 방법.
 여기서, Δy 는 인접 정수 데이터 간 차의 최소값을 의미함.

청구항 3

제1항에 있어서,
 상기 조작 추정 실수의 구간을 도출하는 단계는,
 상기 제어부가 상기 정수 데이터의 역산된 데이터를 정의하는 단계;
 상기 제어부가 상기 역산된 데이터에 라운드 함수(round)를 적용하여 복원 데이터를 계산하는 단계; 및
 상기 제어부가 상기 복원 데이터의 모든 항목에 대해 상기 탐색 범위에 속하는 조작 추정 실수의 구간을 각각 도출하는 단계를 포함하는 것을 특징으로 하는 데이터 조작 감지 방법.

청구항 4

제3항에 있어서,
 상기 탐색 범위에 속하는 조작 추정 실수의 구간을 각각 도출하는 단계에서,
 상기 제어부는, 상기 역산된 데이터와 상기 복원 데이터의 모든 항목에 대해 두 데이터 간의 차이가 $1/(2 \times \text{조작 추정 실수})$ 이하인 조건을 만족하는 조작 추정 실수의 구간을 추정하는 것을 특징으로 하는 데이터 조작 감지 방법.

청구항 5

제4항에 있어서,
 상기 정수 데이터의 조작 여부를 판단하는 단계에서,
 상기 제어부는, 상기 복원 데이터의 모든 항목에 대해 도출된 조작 추정 실수 구간의 교집합에 기초하여 상기

정수 데이터의 조작 여부를 판단하는 것을 특징으로 하는 데이터 조작 감지 방법.

청구항 6

제5항에 있어서,

상기 정수 데이터의 조작 여부를 판단하는 단계에서,

상기 제어부는, 상기 조작 추정 실수의 구간에 교집합이 존재하는 경우 상기 정수 데이터를 조작된 데이터로 판단하고, 교집합이 공집합인 경우 상기 정수 데이터를 조작되지 않은 데이터로 판단하는 것을 특징으로 하는 데이터 조작 감지 방법.

청구항 7

정수로 구성된 정수 데이터에 대해, 각 정수 데이터 간의 차를 활용하여 탐색 범위를 축소하는 탐색 범위 설정부;

상기 축소된 탐색 범위에서 조작에 사용된 것으로 추정되는 조작 추정 실수의 구간을 도출하는 조작 추정 실수 구간 도출부; 및

상기 제어부가 상기 도출된 조작 추정 실수의 구간에 기초하여 상기 정수 데이터의 조작 여부를 판단하는 판단부

를 포함하는 데이터 조작 감지 장치.

청구항 8

제7항에 있어서,

상기 탐색 범위 설정부는, $2\log \Delta y$ 로 탐색 범위를 축소하는 것을 특징으로 하는 데이터 조작 감지 장치.

여기서, Δy 는 인접 정수 데이터 간 차의 최소값을 의미함.

청구항 9

제7항에 있어서,

상기 조작 추정 실수 구간 도출부는,

상기 정수 데이터의 역산된 데이터를 정의하고, 상기 역산된 데이터에 라운드 함수(round)를 적용하여 복원 데이터를 계산하며, 상기 복원 데이터의 모든 항목에 대해 상기 탐색 범위에 속하는 조작 추정 실수의 구간을 각각 도출하는 것을 특징으로 하는 데이터 조작 감지 장치.

청구항 10

제9항에 있어서,

상기 조작 추정 실수 구간 도출부는,

상기 역산된 데이터와 상기 복원 데이터의 모든 항목에 대해 두 데이터 간의 차이가 $1/(2 \times \text{조작 추정 실수})$ 이 하인 조건을 만족하는 조작 추정 실수의 구간을 추정하는 것을 특징으로 하는 데이터 조작 감지 장치.

청구항 11

제10항에 있어서,

상기 판단부는, 상기 복원 데이터의 모든 항목에 대해 도출된 조작 추정 실수 구간의 교집합에 기초하여 상기 정수 데이터의 조작 여부를 판단하는 것을 특징으로 하는 데이터 조작 감지 장치.

청구항 12

제11항에 있어서,

상기 판단부는, 상기 조작 추정 실수의 구간에 교집합이 존재하는 경우 상기 정수 데이터를 조작된 데이터로 판단하고, 교집합이 공집합인 경우 상기 정수 데이터를 조작되지 않은 데이터로 판단하는 것을 특징으로 하는 데이터 조작 감지 장치.

발명의 설명

기술 분야

[0001] 본 발명은 데이터 조작 감지 방법 및 장치에 관한 것으로서, 보다 상세하게는 정수로 구성된 정수데이터에 대해 실수 곱셈 연산과 반올림 연산을 통해 조작된 데이터인지 판단할 수 있는 데이터 조작 감지 방법 및 장치에 관한 것이다.

배경 기술

[0002] 사회적/경제적으로 영향을 끼칠 수 있는 정량적 데이터의 경우 적절한 절차를 통해 검증을 거쳐야 하지만, 사실 기관에서 발표하는 데이터들의 경우 검증하기 어려운 경우가 많다.

[0003] 특히 주관 기관에서 공표한 데이터만을 바탕으로 조작 여부를 판단하는 것은 데이터 취합 과정에서 관련 정보 없이 진행하게 되기 때문에 검증 과정에 있어서 기술적인 어려움이 존재하며, 정확도 측면에서 한계가 있을 수 있다.

[0004] 이러한 공공 데이터의 대표적인 사례로 투표가 있는데, 공공 기관에서 주관하는 투표의 경우 전반적인 과정 및 결과에 대한 검증을 담당하는 전담 기구가 있는 경우가 있으나, 해외 사례에서는 이러한 전담 기구의 존재에도 불구하고 투표의 조작에 대한 의혹이 제기되는 경우도 있다.

[0005] 데이터만을 활용한 투표 검증 기법은 크게 2가지가 있으며, 첫 번째는 Benfold 법칙을 활용한 검증 방법이며, 두 번째는 데이터의 분포를 기반으로 한 검증 방법이다. Benfold의 법칙을 활용한 검증 방법의 경우, 과거의 일부 데이터에 대해서는 조작 여부를 구분할 수 있으나, 타 기관에서의 교차 검증 과정에서 데이터에 따라 조작 여부를 정확하게 판단하지 못하는 단점이 있다. 데이터 분포를 기반으로 한 검증 방법은 데이터의 분포에 의존한 방법으로써, 일부 데이터만 조작되어 기존의 데이터 분포가 바뀌는 경우에 특화된 검출 기법이다. 이 방법은 전체 데이터를 일괄적으로 곱셈을 통해 조작할 경우, 데이터의 분포 형태는 그대로 유지되므로 데이터의 조작 여부 검출에 어려움이 있다.

[0006] 따라서 투표와 같이 전체 값이 정수인 데이터가 일괄적인 곱셈으로 부풀려졌을 때는 분포에 의한 검증이 불가능하며, 특히 정수가 아닌 실수를 곱한 후 반올림을 적용하게 되면 최대 공약수를 찾는 방법으로는 조작 여부를 알아내거나 조작에 사용된 실수를 찾아내기 어렵다.

[0007] 본 발명의 배경기술로는 대한민국 등록특허공보 제10-1962686호(2019.03.27. 공고)인 "전자 투표 시스템 및 방법"이 있다.

발명의 내용

해결하려는 과제

[0008] 본 발명은 전술한 문제점을 개선하기 위하여 안출된 것으로, 본 발명의 일 측면에 따른 목적은 정수로 구성된

정수데이터에 대해 실수 곱셈 연산과 반올림 연산을 통해 조작된 데이터인지 판단할 수 있도록 하는 데이터 조작 감지 방법 및 장치를 제공하는 것이다.

[0009] 본 발명이 해결하고자 하는 과제는 이상에서 언급한 과제(들)로 제한되지 않으며, 언급되지 않은 또 다른 과제(들)은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0010] 본 발명의 일 측면에 따른 데이터 조작 감지 방법은, 제어부가 정수로 구성된 정수 데이터에 대해, 각 정수 데이터 간의 차를 활용하여 탐색 범위를 축소하는 단계, 상기 제어부가 상기 축소된 탐색 범위에서 조작에 사용된 것으로 추정되는 조작 추정 실수의 구간을 도출하는 단계, 및 상기 제어부가 상기 도출된 조작 추정 실수의 구간에 기초하여 상기 정수 데이터의 조작 여부를 판단하는 단계를 포함한다.

[0011] 본 발명은 상기 탐색 범위를 축소하는 단계에서, 상기 제어부는, $2\log \Delta y$ 로 탐색 범위를 축소할 수 있다.

[0012] 본 발명에서 상기 조작 추정 실수의 구간을 도출하는 단계는, 상기 제어부가 상기 정수 데이터의 역산된 데이터를 정의하는 단계, 상기 제어부가 상기 역산된 데이터에 라운드 함수(round)를 적용하여 복원 데이터를 계산하는 단계, 상기 제어부가 상기 복원 데이터의 모든 항목에 대해 상기 탐색 범위에 속하는 조작 추정 실수의 구간을 각각 도출하는 단계를 포함할 수 있다.

[0013] 본 발명은 상기 탐색 범위에 속하는 조작 추정 실수의 구간을 각각 도출하는 단계에서, 상기 제어부는, 상기 역산된 데이터와 상기 복원 데이터의 모든 항목에 대해 두 데이터 간의 차이가 $1/(2 \times \text{조작 추정 실수})$ 이하인 조건을 만족하는 조작 추정 실수의 구간을 추정할 수 있다.

[0014] 본 발명은 상기 정수 데이터의 조작 여부를 판단하는 단계에서, 상기 제어부는, 상기 복원 데이터의 모든 항목에 대해 도출된 조작 추정 실수 구간의 교집합에 기초하여 상기 정수 데이터의 조작 여부를 판단할 수 있다.

[0015] 본 발명은 상기 정수 데이터의 조작 여부를 판단하는 단계에서, 상기 제어부는, 상기 조작 추정 실수의 구간에 교집합이 존재하는 경우 상기 정수 데이터를 조작된 데이터로 판단하고, 교집합이 공집합인 경우 상기 정수 데이터를 조작되지 않은 데이터로 판단할 수 있다.

[0016] 본 발명의 다른 측면에 따른 데이터 조작 감지 장치는, 정수로 구성된 정수 데이터에 대해, 각 정수 데이터 간의 차를 활용하여 탐색 범위를 축소하는 탐색 범위 설정부, 상기 축소된 탐색 범위에서 조작에 사용된 것으로 추정되는 조작 추정 실수의 구간을 도출하는 조작 추정 실수 구간 도출부, 및 상기 제어부가 상기 도출된 조작 추정 실수의 구간에 기초하여 상기 정수 데이터의 조작 여부를 판단하는 판단부를 포함한다.

[0017] 본 발명에서 상기 탐색 범위 설정부는, $2\log \Delta y$ 로 탐색 범위를 축소할 수 있다.

[0018] 본 발명에서 상기 조작 추정 실수 구간 도출부는, 상기 정수 데이터의 역산된 데이터를 정의하고, 상기 역산된 데이터에 라운드 함수(round)를 적용하여 복원 데이터를 계산하며, 상기 복원 데이터의 모든 항목에 대해 상기 탐색 범위에 속하는 조작 추정 실수의 구간을 각각 도출할 수 있다.

[0019] 본 발명에서 상기 조작 추정 실수 구간 도출부는, 상기 역산된 데이터와 상기 복원 데이터의 모든 항목에 대해 두 데이터 간의 차이가 $1/(2 \times \text{조작 추정 실수})$ 이하인 조건을 만족하는 조작 추정 실수의 구간을 추정할 수 있다.

[0020] 본 발명에서 상기 판단부는, 상기 복원 데이터의 모든 항목에 대해 도출된 조작 추정 실수 구간의 교집합에 기초하여 상기 정수 데이터의 조작 여부를 판단할 수 있다.

[0021] 본 발명에서 상기 판단부는, 상기 조작 추정 실수의 구간에 교집합이 존재하는 경우 상기 정수 데이터를 조작된 데이터로 판단하고, 교집합이 공집합인 경우 상기 정수 데이터를 조작되지 않은 데이터로 판단할 수 있다.

발명의 효과

[0022] 본 발명의 일 실시예에 따른 데이터 조작 감지 방법 및 장치는, 정수로 구성된 정수데이터에 대해 실수 곱셈 연산과 반올림 연산을 통해 조작된 데이터인지 판단할 수 있다.

[0023] 본 발명의 다른 실시예에 따른 데이터 조작 감지 방법 및 장치는, 정수 데이터에 대해 조작에 사용된 실수 곱셈

을 역으로 추적하는 과정에서 발생할 수 있는 다수의 실수 연산과 나머지 연산에 대해서 속도 측면에서 효율적으로 수행할 수 있다.

[0024] 한편, 본 발명의 효과는 이상에서 언급한 효과들로 제한되지 않으며, 이하에서 설명할 내용으로부터 통상의 기술자에게 자명한 범위 내에서 다양한 효과들이 포함될 수 있다.

도면의 간단한 설명

[0025] 도 1은 본 발명의 일 실시예에 따른 정수 데이터의 조작 규명 방법을 설명하기 위한 개념도이다.

도 2는 본 발명의 일 실시예에 따른 데이터 조작 감지 장치를 설명하기 위한 블록도이다.

도 3은 본 발명의 일 실시예에 따른 데이터 조작 감지 방법을 설명하기 위한 흐름도이다.

도 4는 본 발명의 일 실시예에 따른 역산 과정에서 도출 가능한 조작 추정 실수가 해가 되는 조건을 설명하기 위한 도면이다.

도 5는 본 발명의 일 실시예에 따른 정수 조건을 활용한 조작 추정 실수의 탐색 과정을 설명하기 위한 도면이다.

도 6은 본 발명의 일 실시예에 따른 탐색 범위 내 조작 추정 실수의 구간을 구하기 위한 과정을 설명하기 위한 도면이다.

도 7은 본 발명의 일 실시예에 따른 데이터 조작 감지를 위한 알고리즘을 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

[0026] 이하, 첨부된 도면들을 참조하여 본 발명의 일 실시예에 따른 데이터 조작 감지 방법 및 장치를 설명한다. 이 과정에서 도면에 도시된 선들의 두께나 구성요소의 크기 등은 설명의 명료성과 편의상 과장되게 도시되어 있을 수 있다.

[0027] 또한, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례에 따라 달라질 수 있다. 그러므로 이러한 용어들에 대한 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0028] 또한, 본 명세서에서 설명된 구현은, 예컨대, 방법 또는 프로세스, 장치, 소프트웨어 프로그램, 데이터 스트림 또는 신호로 구현될 수 있다. 단일 형태의 구현의 맥락에서만 논의(예컨대, 방법으로서만 논의)되었더라도, 논의된 특징의 구현은 또한 다른 형태(예컨대, 장치 또는 프로그램)로도 구현될 수 있다. 장치는 적절한 하드웨어, 소프트웨어 및 펌웨어 등으로 구현될 수 있다. 방법은, 예컨대, 컴퓨터, 마이크로프로세서, 집적 회로 또는 프로그래밍 가능한 로직 디바이스 등을 포함하는 프로세싱 디바이스를 일반적으로 지칭하는 프로세서 등과 같은 장치에서 구현될 수 있다. 프로세서는 또한 최종-사용자 사이에 정보의 통신을 용이하게 하는 컴퓨터, 셀 폰, 휴대용/개인용 정보 단말기(personal digital assistant: "PDA") 및 다른 디바이스 등과 같은 통신 디바이스를 포함한다.

[0030] 도 1은 본 발명의 일 실시예에 따른 정수 데이터의 조작 규명 방법을 설명하기 위한 개념도이다.

[0031] 도 1을 참조하면, 정수로 구성된 정수 데이터(Y)를 사용자로부터 입력받으면, 데이터 조작 감지 장치(100)는 정수 데이터(Y)의 조작 여부를 판단할 수 있다. 이를 위해, 데이터 조작 감지 장치(100)는 다른 정수로 구성된 데이터(Z)에 곱셈과 나머지 연산을 적용하여 입력받은 정수 데이터(Y)가 도출될 수 있는 실수들(α)을 찾는다. 이 과정에서 연속적으로 값이 존재하는 실수 영역에서는 일반적인 방법으로 원하는 값을 탐색하기 위해 근사법을 활용하거나 단순한 대입법을 활용한 접근이 필요하기에 탐색 정확도 혹은 연산 속도 측면에서 한계가 있다.

[0032] 이에, 본 발명은 정수로 구성된 데이터라는 특징을 활용하여 탐색 영역을 정수 영역으로 변환함으로써 한정된 수의 연산만으로 조작 여부와 조작에 사용된 실수가 존재할 수 있는 구간을 도출할 수 있다.

[0034] 도 2는 본 발명의 일 실시예에 따른 데이터 조작 감지 장치를 설명하기 위한 블록도이다.

[0035] 도 2를 참조하면, 본 발명의 일 실시예에 따른 데이터 조작 감지 장치(100)는 인터페이스부(110), 메모리(120),

및 제어부(130)를 포함한다.

- [0036] 인터페이스부(110)는 사용자로부터 정수로 구성된 정수 데이터를 입력받는 역할을 수행할 수 있다. 이때 인터페이스부(110)는 다른 네트워크 장치와 유무선 연결을 통해 제어 신호 또는 데이터 신호와 같은 신호를 송수신하기 위해 필요한 하드웨어 및 소프트웨어를 포함하는 장치일 수 있다. 또한, 인터페이스부(110)는 근거리 통신모듈, 무선 통신모듈, 이동통신 모듈, 유선 통신모듈 등 다양한 형태로 구현될 수 있다.
- [0037] 메모리(120)는 데이터 조작 감지 장치(100)의 동작과 관련된 데이터들을 저장하는 구성이다. 여기서 메모리(120)는 공지된 저장매체를 이용할 수 있으며, 예를 들어, ROM, PROM, EPROM, E EPROM, RAM 등과 같이 공지된 저장매체 중 어느 하나 이상을 이용할 수 있다. 특히, 메모리(120)에는 정수 데이터 조작 감지를 위한 알고리즘(프로그램, 애플리케이션 또는 애플릿) 등이 저장될 수 있으며, 저장되는 정보들은 필요에 따라 제어부(130)에 의해 취사선택될 수 있다.
- [0038] 제어부(130)는 인터페이스부(110)로부터 정수 데이터를 입력받으면, 정수로 구성된 데이터라는 특징을 활용하여 탐색 영역을 정수 영역으로 변환하고, 이를 통해 한정된 수의 연산만으로 정수 데이터의 조작 여부와 조작에 사용된 것으로 추정되는 실수(α , 이하 '조작 추정 실수'라 칭함)가 존재할 수 있는 구간을 도출할 수 있다. 여기서, 조작 추정 실수는 정수 데이터의 원본 데이터에 대해 곱셈 연산 또는 반올림 연산을 통해 조작에 사용된 것으로 추정된 실수를 의미할 수 있다.
- [0039] 이러한 제어부(130)는 탐색 범위 설정부(132), 조작 추정 실수 구간 도출부(134), 및 판단부(136)를 포함할 수 있다.
- [0040] 탐색 범위 설정부(132)는 입력받은 정수 데이터에 대해, 각 정수 데이터 간의 차를 활용하여 탐색 범위를 축소할 수 있다. 이때 탐색 범위 설정부(132)는 $2 \log \Delta y$ 로 탐색 범위를 축소할 수 있다.
- [0041] 조작 추정 실수 구간 도출부(134)는 탐색 범위 설정부(132)를 통해 축소된 탐색 범위에서 조작에 사용된 것으로 추정되는 조작 추정 실수의 구간을 도출한다. 이때 조작 추정 실수 구간 도출부(134)는 정수 데이터의 역산된 데이터를 정의하고, 역산된 데이터에 라운드 함수(round)를 적용하여 복원 데이터를 계산하며, 복원 데이터의 모든 항목에 대해 탐색 범위에 속하는 조작 추정 실수의 구간을 각각 도출할 수 있다. 즉, 조작 추정 실수 구간 도출부(134)는 실수 영역의 탐색 범위를 y축의 구간 내에 존재하는 정수들만 찾도록 정수 영역으로 변환할 수 있다. 이를 통해 조작 추정 실수 구간 도출부(134)는 한정된 수의 연산만으로 정수 데이터의 조작 여부와 조작에 사용된 것으로 추정되는 조작 추정 실수가 존재할 수 있는 구간을 도출할 수 있다.
- [0042] 판단부(136)는 실수 구간 도출부(134)에서 조작 추정 실수 구간 도출부(134)에서 도출된 조작 추정 실수의 구간에 기초하여 정수 데이터의 조작 여부를 판단한다. 이때 판단부(136)는 복원 데이터의 모든 항목에 대해 도출된 조작 추정 실수 구간의 교집합에 기초하여 정수 데이터의 조작 여부를 판단할 수 있다. 구체적으로, 판단부(136)는, 조작 추정 실수의 구간에 교집합이 존재하는 경우 정수 데이터를 조작된 데이터로 판단할 수 있고, 교집합이 공집합인 경우 정수 데이터를 조작되지 않은 데이터로 판단할 수 있다.
- [0043] 제어부(130)의 동작에 대한 상세한 설명은 도 3을 참조하기로 한다.
- [0044] 상기와 같이 구성된 제어부(130)는 데이터 조작 감지 장치(100)의 다양한 구성부들의 동작을 제어하는 구성으로, 적어도 하나의 연산 장치를 포함할 수 있는데, 여기서 상기 연산 장치는 범용적인 중앙연산장치(CPU), 특정 목적에 적합하게 구현된 프로그래머블 디바이스 소자(CPLD, FPGA), 주문형 반도체 연산장치(ASIC) 또는 마이크로 컨트롤러 칩일 수 있다. 또한, 다른 형태의 하드웨어로 구현될 수도 있음을 본 실시 예가 속하는 기술분야에서 통상의 지식을 가진 자라면 이해할 수 있다.
- [0045] 제어부(130)는 일종의 중앙처리장치로서 프로그램 메모리(120)에 탑재된 제어 소프트웨어를 구동하는 등의 다양한 기능을 제공할 수 있다. 여기서, 제어부(130)는 프로세서(processor)와 같이 데이터를 처리할 수 있는 모든 종류의 장치를 포함할 수 있다. 여기서, '프로세서(processor)'는, 예를 들어 프로그램 내에 포함된 코드 또는 명령으로 표현된 기능을 수행하기 위해 물리적으로 구조화된 회로를 갖는, 하드웨어에 내장된 데이터 처리 장치를 의미할 수 있다. 이와 같이 하드웨어에 내장된 데이터 처리 장치의 일 예로써, 마이크로프로세서(microprocessor), 중앙처리장치(central processing unit: CPU), 프로세서 코어(processor core), 멀티프로세서(multiprocessor), ASIC(application-specific integrated circuit), FPGA(field programmable gate array) 등의 처리 장치를 망라할 수 있으나, 본 발명의 범위가 이에 한정되는 것은 아니다.

[0047] 도 3은 본 발명의 일 실시예에 따른 데이터 조작 감지 방법을 설명하기 위한 흐름도, 도 4는 본 발명의 일 실시예에 따른 역산 과정에서 도출 가능한 조작 추정 실수가 해가 되는 조건을 설명하기 위한 도면, 도 5는 본 발명의 일 실시예에 따른 정수 조건을 활용한 조작 추정 실수의 탐색 과정을 설명하기 위한 도면, 도 6은 본 발명의 일 실시예에 따른 탐색 범위 내 조작 추정 실수의 구간을 구하기 위한 과정을 설명하기 위한 도면, 도 7은 본 발명의 일 실시예에 따른 데이터 조작 감지를 위한 알고리즘을 나타낸 도면이다.

[0048] 도 3을 참조하면, 정수로 구성된 정수 데이터가 입력되면(S310), 제어부(130)는 각 정수 데이터 간의 차를 활용하여 탐색 범위를 축소한다(S320).

[0049] 이때 제어부(130)는 각 정수 데이터가 특정 실수의 배수일 경우 인접 데이터 간의 차 역시 배수가 된다는 성질을 이용하여 조작에 사용된 것으로 추정되는 실수(α , 이하 ‘조작 추정 실수’라 칭함)를 탐색할 범위를 축소할 수 있다. 여기서, 조작 추정 실수는 정수 데이터의 원본 데이터에 대해 곱셈 연산 또는 반올림 연산을 통해 조작에 사용된 것으로 추정된 실수를 의미할 수 있다. 예를 들어, 정수 데이터가 도 1에 도시된 Y이고, 2배 이상으로 값을 조작한 것으로 가정할 경우, 탐색 범위는 2이상 인접 데이터간의 차(Δy_i)의 최소값 이하로 축소될 수 있다. 즉, 탐색 범위는 $2 \leq \alpha \leq \Delta y_i$ 로 축소될 수 있다.

[0050] 또한 제어부(130)는 조작 추정 실수(α)의 조건을 활용하여 탐색 범위를 축소할 수 있다. 즉, 조작 추정 실수(α)는 정수 데이터(Y)의 원본 데이터(X)에 곱셈 연산 또는 반올림 연산을 통해 조작에 사용된 실수를 의미하므로, 조작 추정 실수(α)의 조건을 생각해보면 $\Delta y - 1 \leq \alpha \Delta x \leq \Delta y + 1$ 로부터 아래 수학적 1과 같은 조작 추정 실수를 확인할 수 있다.

[0051] [수학적 1]

$$\frac{\Delta y - 1}{\Delta x} \leq \alpha \leq \frac{\Delta y + 1}{\Delta x}$$

[0052]

[0053] 여기서, Δy 는 정수 데이터에서 인접 데이터 간의 최소값, Δx 는 원본 데이터에서 인접 데이터간의 차를 의미할 수 있다.

[0054] 수학적 1에서 Δx 를 양의 정수 ℓ 로 설정하면, 양의 정수 ℓ 에 대하여 α_s 와 α_t 를 아래 수학적 2와 같이 정의할 수 있다.

[0055] [수학적 2]

$$\alpha_s = \frac{\Delta y - 1}{\ell} \quad \text{and} \quad \alpha_t = \frac{\Delta y + 1}{\ell}.$$

[0056]

[0057] ℓ 의 범위는 1부터 $(\Delta y - 1)/2$ 을 반올림한 숫자까지가 되므로, 탐색하게 되는 구간을 근사해보면 $2 \log \Delta y$ 가 되는 것을 알 수 있으며, 이는 일정 크기 이상의 Δy 에 대해서 훨씬 축소되는 것을 알 수 있다. 따라서 탐색 범위(I)는 아래 수학적 3과 같이 정의할 수 있다.

[0058] [수학적 3]

$$|I| = \sum_{\ell=1}^{\lceil \frac{\Delta y - 1}{2} \rceil} \frac{2}{\ell} \approx 2 \log \Delta y$$

[0059]

[0060] S320 단계가 수행되면, 제어부(130)는 축소된 탐색 범위(I)에서 모든 조작 추정 실수를 포함하는 구간을 도출한다(S330). 이때 제어부(130)는 정수 데이터의 역산된 데이터를 정의하고, 역산된 데이터에 라운드 함수(round)를 적용하여 복원 데이터를 계산하며, 복원 데이터의 모든 항목에 대해 탐색 범위에 속하는 전체 조작 추정 실

수 구간을 도출할 수 있다.

[0061] 예를 들어, 도 1과 같이 입력받은 정수 데이터 Y에서 조작 추정 실수 α 를 구하고자 할 경우, 제어부(130)는 아래 수학적 식 4와 같이 역산된 값(Z)을 정의할 수 있다.

[0062] [수학적 식 4]

$$\tilde{z}_i := \frac{y_i}{\alpha} \quad \text{and} \quad z_i := \text{round}(\tilde{z}_i)$$

[0063]

[0064] 여기서, $\tilde{z}_i$ 는 역산된 데이터, z_i 는 복원 데이터를 의미할 수 있다.

[0065] 이때 도 4를 참조하여 입력된 데이터와 계산된 데이터 사이의 관계를 살펴보면, 역산된 값과 역산하여 반올림한

값의 차이는 $\frac{1}{2\alpha}$ 보다 작아야 함을 확인할 수 있다. 즉, 역산된 데이터와 복원 데이터 간의 차이는 아래 수학적 식 5와 같이 정의할 수 있다.

[0066] [수학적 식 5]

$$-\frac{1}{2\alpha} < \tilde{z}_i - z_i \leq \frac{1}{2\alpha}$$

[0067]

[0068] 한편, 모든 조작 추정 실수는 수학적 식 3에서 정의된 탐색 범위(I)에 포함되어 있으므로, 제어부(130)는 수학적 식 5를 이용하여 탐색 범위(I)에서 조작 추정 실수를 추정할 수 있다. 그러나 연속적으로 값이 존재하는 실수 영역에서는 일반적인 방법으로 원하는 값을 탐색하기 위해 근사법을 활용하거나 단순한 대입법을 활용한 접근이 필요하기에 탐색 정확도 혹은 연산 속도 측면에서 한계가 있다. 즉, 단순하게 접근하는 경우 조작 추정 실수의 탐색은 도 5의 X축 방향으로 진행하게 되므로, 조건을 만족하는 실수 범위를 찾기 위해 많은 노력이 필요하다.

[0069] 이에, 본 발명은 정수로 구성된 데이터라는 특징을 활용하여 탐색 영역을 정수 영역으로 변환함으로써 한정된 수의 연산만으로 정수 데이터의 조작 여부와 조작에 사용된 실수가 존재할 수 있는 구간을 도출할 수 있다.

[0070] 즉, 수학적 식 5를 z_i 로 정리하면, $\tilde{z} - 1/(2\alpha) \leq z_i < \tilde{z}_i + 1/(2\alpha)$ 일 수 있고, 이 수학적 식에 수학적 식 4를 적용하면, 수학적 식 5는 아래 수학적 식 6과 같이 정의할 수 있다.

[0071] [수학적 식 6]

$$f_i^-(\alpha) \leq z_i < f_i^+(\alpha)$$

[0072]

[0073] 여기서, $f_i^-(\alpha) = \frac{y_i - 0.5}{\alpha}$, $f_i(\alpha) = \frac{y_i}{\alpha}$ and $f_i^+(\alpha) = \frac{y_i + 0.5}{\alpha}$ 일 수 있고, 도 4에 도시된 그래프와 같이 정의할 수 있다.

[0074] 제어부(130)는 실수 영역의 탐색 범위를 도 5에 도시된 바와 같이 y축의 구간 내에 존재하는 정수들만 찾도록 정수 영역으로 변환할 수 있다. 본 발명은 y축의 구간 내에 존재하는 정수들만 찾는 형태로 진행함으로써, 연산 속도를 빠르게 할 수 있다.

[0075] 예를 들어, 도 6의 경우 전체 데이터 중 i번째 항목에 대해 주어진 조건을 만족하는 조작 추정 실수(α)의 구간이므로, 제어부(130)는 모든 데이터 항목에 대해 이를 만족하는 조작 추정 실수(α)의 구간을 찾아서 교집합을 구함으로써, 조작 추정 실수(α)의 구간을 찾을 수 있다.

[0076] S330 단계가 수행되면, 제어부(130)는 모든 데이터 항목에 대해 주어진 조건을 만족하는 조작 추정 실수(α)의 구간을 찾아서 교집합이 존재하는지를 판단한다(S340).

[0077] S340 단계의 판단결과, 교집합이 존재하면, 제어부(130)는 정수 데이터를 조작된 데이터로 판단한다(S350).

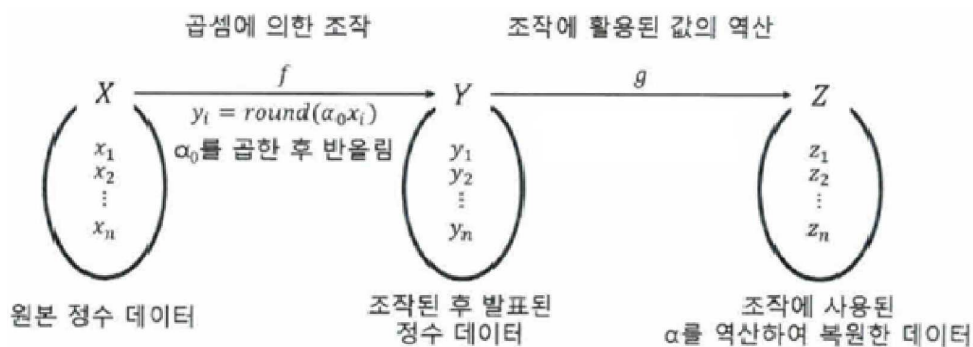
- [0078] 만약 S340 단계의 판단결과, 교집합이 존재하지 않으면, 제어부(130)는 정수 데이터를 조작되지 않은 데이터로 판단한다(S360).
- [0079] 상술한 과정을 알고리즘으로 표현하면, 도 6과 같을 수 있다.
- [0080] 도 7에 도시된 알고리즘은 전체 데이터들에 대해 주어진 조건을 만족하는 α 의 구간을 찾아서 교집합을 구하게 되므로, 조작되지 않은 데이터에 대해 가장 많은 수의 연산이 필요하다.
- [0081] 본 발명에서는 데이터의 각 항목에 대해 α 의 구간을 찾을 때 가장 멀리 떨어진 첫 번째 항목과 마지막 항목을 가장 먼저 대조함으로써, 교집합을 보다 빠른 시점에 찾을 수 있다. 이러한 순서를 활용할 경우, 빠르게 주어진 조건을 만족하지 않는 것을 확인함으로써 조기에 연산을 종료할 수 있다.
- [0083] 상술한 바와 같이 본 발명의 일 실시예에 따른 데이터 조작 감지 방법 및 장치는, 정수로 구성된 정수데이터에 대해 실수 곱셈 연산과 반올림 연산을 통해 조작된 데이터인지 판단할 수 있다.
- [0084] 본 발명의 다른 실시예에 따른 데이터 조작 감지 방법 및 장치는, 정수 데이터에 대해 조작에 사용된 실수 곱셈을 역으로 추적하는 과정에서 발생할 수 있는 다수의 실수 연산과 나머지 연산에 대해서 속도 측면에서 효율적으로 수행할 수 있다.
- [0085] 본 발명은 도면에 도시된 실시예를 참고로 하여 설명되었으나, 이는 예시적인 것에 불과하며, 당해 기술이 속하는 분야에서 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서 본 발명의 진정한 기술적 보호범위는 아래의 특허청구범위에 의해서 정하여져야 할 것이다.

부호의 설명

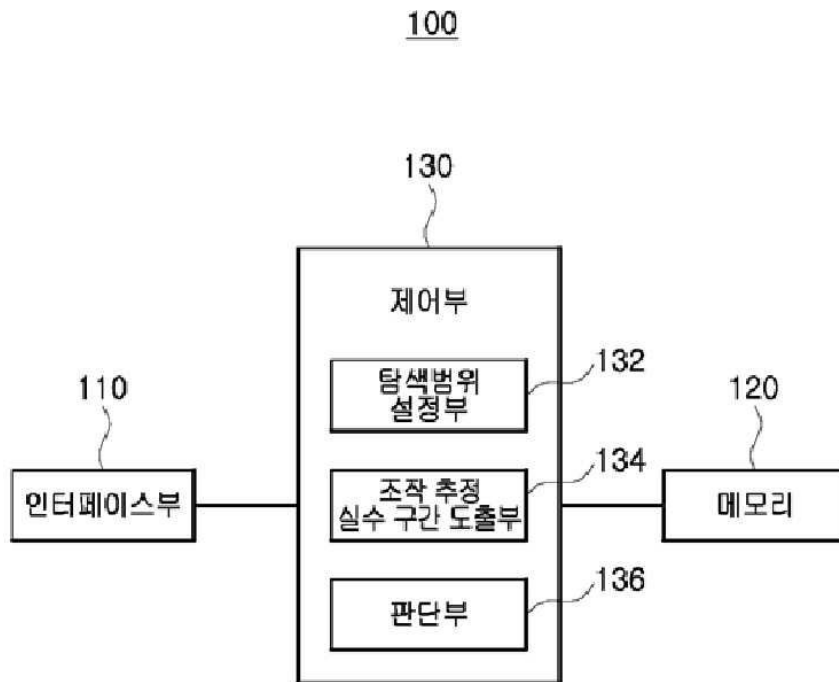
- [0086] 100 : 데이터 조작 감지 장치
- 110 : 인터페이스부
- 120 : 메모리
- 130 : 제어부
- 132 : 탐색 범위 설정부
- 134 : 조작 추정 실수 구간 도출부
- 136 : 판단부

도면

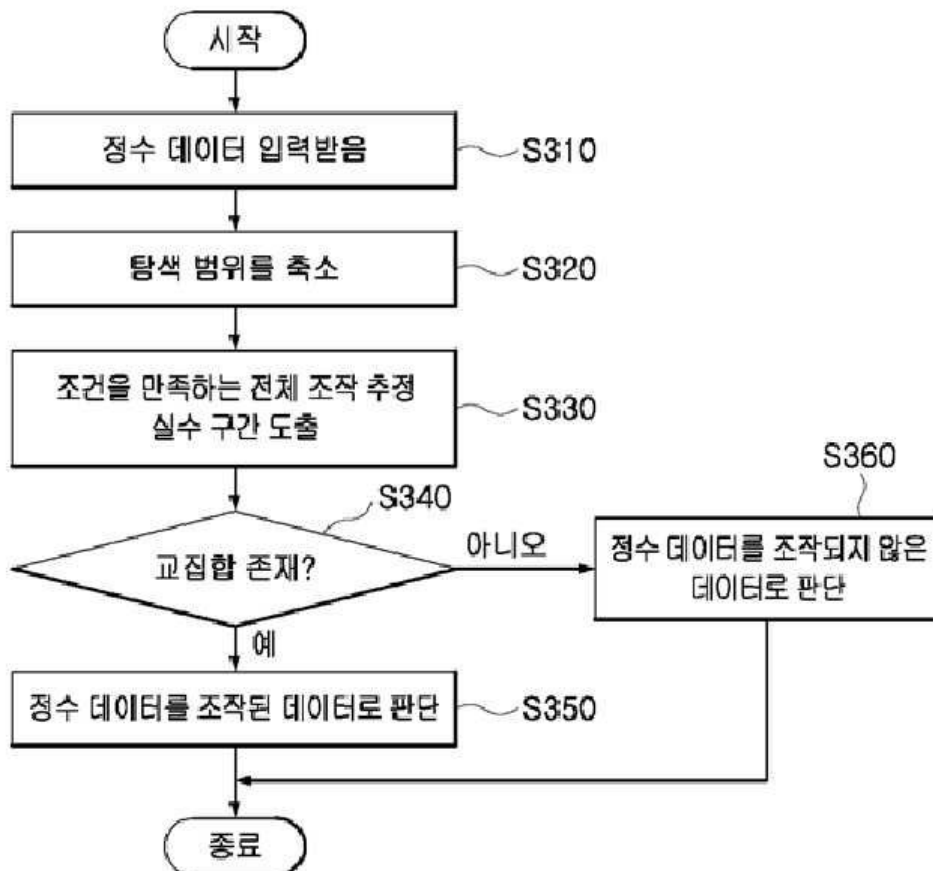
도면1



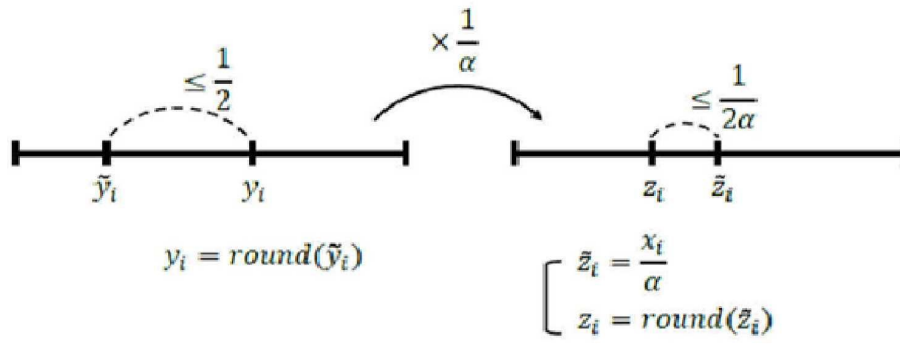
도면2



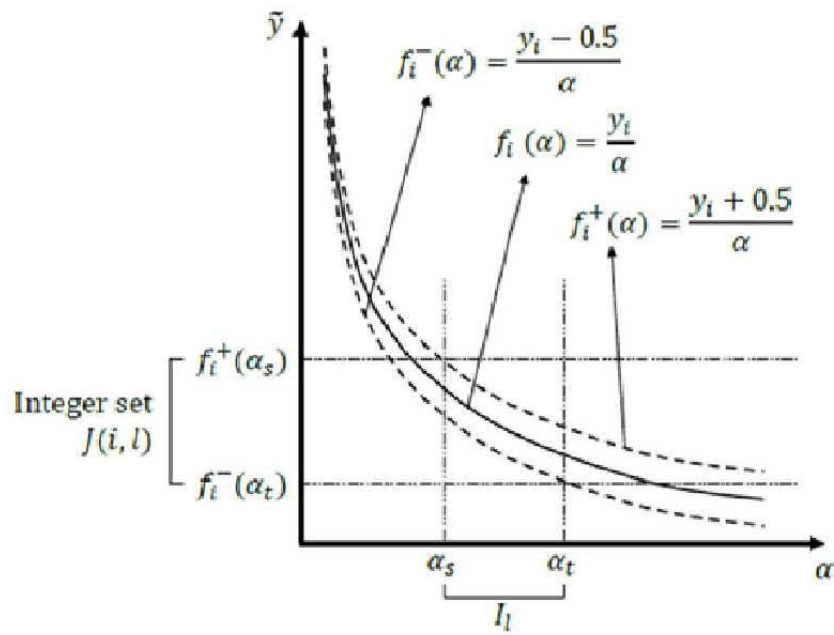
도면3



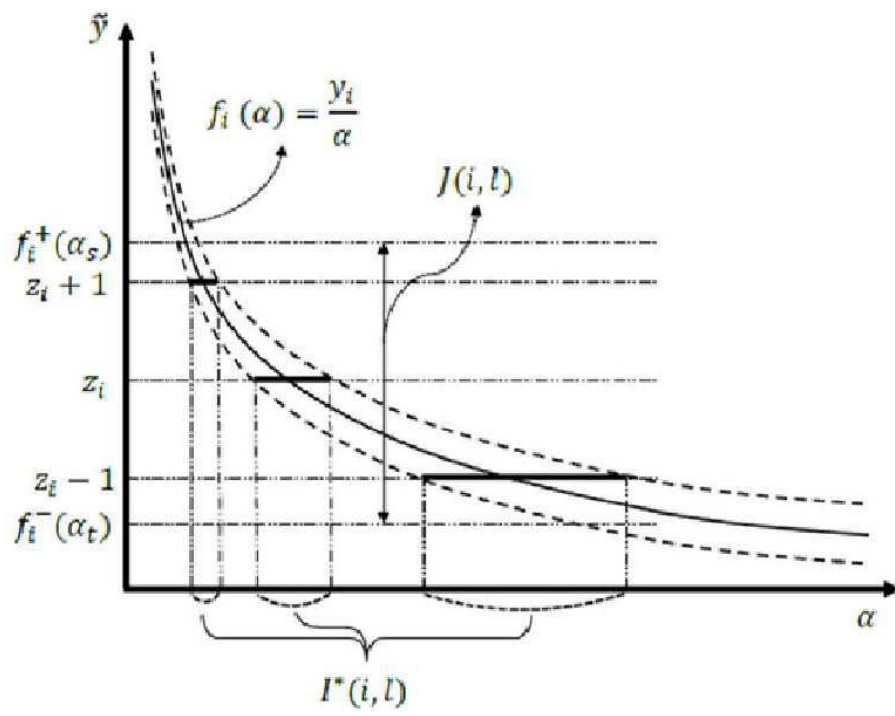
도면4



도면5



도면6



도면7

Input: Ballot counts $\{y_1, \dots, y_n\}$

Output: a flag m indicating whether $\{y_i\}$ is multiplied or unmultiplied,
the rightmost interval I^* of the set of all proper multiplicative factors

```

 $m \leftarrow \text{unmultiplied}$ 
 $I^* \leftarrow \emptyset$ 
 $I_\ell^* \leftarrow \emptyset$ 
if  $\Delta y = 1$  then
    return  $m, I_\ell^*$ 
for  $\ell \leftarrow 1$  to  $\lceil \frac{\Delta y - 1}{2} \rceil$  do
     $\alpha_s \leftarrow \frac{\Delta y - 1}{\ell}, \alpha_l \leftarrow \frac{\Delta y + 1}{\ell}$ 
    if  $\alpha_s < 2$  then
         $\alpha_s \leftarrow 2$ 
     $I_\ell^* \leftarrow [\alpha_s, \alpha_l]$ 
    for  $i \leftarrow 1$  to  $n$  do
         $I^*(i, \ell) \leftarrow \emptyset$ 
         $z_{low} \leftarrow \left\lceil \frac{y_i - 0.5}{\alpha_l} \right\rceil, z_{high} \leftarrow \left\lfloor \frac{y_i + 0.5}{\alpha_s} \right\rfloor$ 
        for  $j \leftarrow z_{low}$  to  $z_{high}$  do
             $I^*(i, \ell) \leftarrow I^*(i, \ell) \cup \left[ \frac{y_i - 0.5}{j}, \frac{y_i + 0.5}{j} \right)$ 
        end for
         $I_\ell^* \leftarrow I_\ell^* \cap I^*(i, \ell)$ 
        if  $I_\ell^* = \emptyset$  then
            break
    end for
    if  $I_\ell^* \neq \emptyset$  then
         $m \leftarrow \text{multiplied}$ 
         $I^* \leftarrow \text{the rightmost interval of } I_\ell^*$ 
        break
end for
return  $m, I^*$ 

```