부호 이론에서의 격자점 열거와 정수계획법

본 연구보고서는 제한된 무게를 가지는 선형 부호의 분류 문제를 격자점 열거와 정수계획법을 통해 해결하는 방법론을 다룬다 .

- **초록**

부호 이론에서 선형 부호의 분류는 기본적인 조합론적 문제이지만, 부호의 매개변수가 커질수록 계산 복잡도가 급증한다. 본 논문은 격자점 열거 알고리즘과 정수계획법(ILP)을 결합하여 제한된 무게 스펙트럼을 가지는 선형 부호를 효율적으로 분류하는 방법을 제시한다 . 특히 정수계획법 공식화를 Phase 0으로 도입하여 격자점 열거 단계에서 불필요한 후보를 사전에 제거함으로써 계산 효율성을 크게 향상시킨다 .

1. **서론**

   선형 부호는 유한체 위의 벡터 부분공간으로, 오류 정정 능력을 특성화하는 최소 해밍 거리(Hamming distance) d를 가진다. 실제 응용에서 특정 무게 스펙트럼을 가지는 부호의 존재 여부는 중요한 문제이다 .

   문제 정의:
   [n,k]_q-부호 C는 유한체 F_q 위의 k-차원 부분공간이며, 부호말(codeword)은 길이 n의 벡터이다. 비자명 부호말의 무게(1인 위치의 개수)는 특정 범위 {aΔ, (a+1)Δ, ..., bΔ}에 제한될 수 있다 .

   부호 분류의 전통적 방법은 생성 행렬 G의 확장을 통한 격자점 열거이다. 체계적 생성 행렬 형태로 기존 부호를 확장하는데, 이때 새로운 행의 계수 패턴은 특정 제약 조건을 만족해야 한다 .

2. **격자점 열거의 기반이 되는 ILP 공식화**

   격자점 열거는 다음의 Diophantine 방정식 시스템을 풀어야 한다 :

   여기서 변수 x_P는 확장된 부호에서 행 공간(row span)이 P인 열의 개수를 나타낸다 .

   이 제약 조건들은 다음을 보장한다 :

   - 무게 조건:
     방정식 (1)은 모든 부호말의 무게가 [aΔ, bΔ] 범위에 있음을 보장한다.
   - 형태 조건:
     방정식 (2)는 생성 행렬의 체계적 형태를 유지한다.
   - 가역성 조건:
     방정식 (3)은 각 기저 벡터가 필요하다.

   전통적 접근법에서는 Phase 1에서 모든 격자점을 열거한 후, Phase 2에서 추가 검사를 수행한다 . 본 연구는 이를 개선하여 ILP를 Phase 0으로 도입한다 .

3. **개선된 Phase 0 ILP 공식화**

   정수계획법을 사용하여 확장 가능성을 사전 검사하면, 격자점 열거의 불필요한 후보를 제거할 수 있다.

   조건부 제약 1 (Canon Length):
   확장을 "정규 길이 확장(canonical length extension)"이라 하면, 최소 출현 열의 개수를 먼저 확인한다. 이를 이진 변수 u_P로 선형화하면...

   조건부 제약 2 (무게 스펙트럼 갭):
   가능한 무게가 여러 구간으로 나뉘어있으면(예: {a_1Δ_1, ..., b_1Δ_1} ∪ {a_2Δ_2, ..., b_2Δ_2}), 다음을 사용한다. 여기서 z_i^H ∈ {0,1}은 각 초평면에서 사용할 무게 범위를 선택한다 .

4. **계산 결과**

   제안된 방법의 효과를 구체적 사례로 보인다 .

   사례 1: 2-무게 부호의 비존재성

   프로젝티브 2-무게 [≤34, 3, {28,32}]_8-부호를 찾는 문제를 고려한다 . Phase 0 ILP 검사를 통해 여러 불가능한 후보를 제거한 후, 격자점 열거를 수행한다.

   결과: 유일한 [34, 3, {28,32}]_8-부호를 발견하였으며, 확장 불가능함을 확인했다. ILP 계산: 5.6시간, 1,633,887개의 분기-한계 노드 검사 .

   사례 2: 대규모 부호 분류

   [74,3,{56,64}]_4-부호에서 [76,4,{56,64}]_4로의 확장을 고려하면, Phase 0 없이는 1,087,803개의 부호가 격자점 열거로 구성되었으나 나중에 제거되었다 . Phase 0 ILP는 이들을 사전에 제거하여 계산 시간을 크게 단축했다.

   결과: 정확히 5개의 동형 불가능한 [76,4,{56,64}]_4-부호를 발견했다 .

   사례 3: Δ-분할가능 부호

   8-분할가능 [n,k]_2-부호의 프로젝티브 버전이 존재하는 길이를 특성화한다 . Phase 0 ILP 공식화:

   여기서 분할가능 조건이 자동으로 고려된다.

5. **방법론의 일반화**

   제안된 Phase 0 ILP 접근법은 다음과 같이 일반화된다 :

   1. 선형 부호 이외의 적용:
      덧셈 부호(additive codes), 비선형 부호에도 확장 가능하다 .

2. 다른 거리 메트릭:
   Lee 거리, Hamming 거리 외 다른 메트릭에도 적용 가능하다 .
3. ILP 솔버의 활용:
   Gurobi, CPLEX와 같은 상용 솔버를 직접 사용하여 격자점 열거 없이 격자점을 세는 것도 가능하다 .

특히 복잡한 제약 조건을 가진 부호의 경우, 전체 ILP를 Phase 1 없이 직접 풀 수도 있다 .

6. 결론

본 논문은 부호 분류 문제에서 정수계획법의 효율적 활용을 보였다. 격자점 열거의 사전 필터링으로서 Phase 0 ILP 공식화는 계산 시간을 수십 배 단축할 수 있다 . 이 방법론은 부호 이론의 여러 조합론적 문제로 확장 가능하며, 대규모 부호 분류의 계산 가능성을 크게 향상시킨다 . 향후 연구는 병렬 처리 및 휴리스틱 접근법과의 결합을 통해 더욱 큰 규모의 부호 분류를 목표로 할 것이다.