Washington State University

Department of Mathematics

Lattice-based Algorithms for Number Partitioning in the Hard Phase

Bala Krishnamoorthy

joint work with

William Webb and Nathan Moyer

Department of Mathematics, WSU

AMS Western Section Meeting, San Francisco

April 25, 2009

Number Partitioning Problem (NPP)

Number Partitioning Problem (NPP)

- Given $S = \{a_1, \ldots, a_n\}$ with $a_j \in \mathbb{Z}_{>0}$, $\alpha = \sum_j a_j$,

Number Partitioning Problem (NPP)

- Given $S = \{a_1, \ldots, a_n\}$ with $a_j \in \mathbb{Z}_{>0}$, $\alpha = \sum_j a_j$,
- divide S into 2 disjoint subsets $S_1 \cup S_2 = S$ such that

Number Partitioning Problem (NPP)

- Given $S = \{a_1, \ldots, a_n\}$ with $a_j \in \mathbb{Z}_{>0}$, $\alpha = \sum_j a_j$,
- divide S into 2 disjoint subsets $S_1 \cup S_2 = S$ such that

$$\triangle = \left| \sum_{j \in S_1} a_j \; - \; \sum_{j \in S_2} a_j \right|,$$

Number Partitioning Problem (NPP)

- Given $S = \{a_1, \ldots, a_n\}$ with $a_j \in \mathbb{Z}_{>0}$, $\alpha = \sum_j a_j$,
- divide S into 2 disjoint subsets $S_1 \cup S_2 = S$ such that

$$\triangle = \left| \sum_{j \in S_1} a_j \; - \; \sum_{j \in S_2} a_j \right|,$$ the *discrepancy*,

Number Partitioning Problem (NPP)

- Given $S = \{a_1, \ldots, a_n\}$ with $a_j \in \mathbb{Z}_{>0}$, $\alpha = \sum_j a_j$,
- divide S into 2 disjoint subsets $S_1 \cup S_2 = S$ such that

$$\triangle = \left| \sum_{j \in S_1} a_j \; - \; \sum_{j \in S_2} a_j \right|,$$ the *discrepancy*,

is minimized.

Number Partitioning Problem (NPP)

- Given $S = \{a_1, \ldots, a_n\}$ with $a_j \in \mathbb{Z}_{>0}$, $\alpha = \sum_j a_j$,
- divide S into 2 disjoint subsets $S_1 \cup S_2 = S$ such that

$$\triangle = \left| \sum_{j \in S_1} a_j \; - \; \sum_{j \in S_2} a_j \right|, \text{ the } \textit{discrepancy},$$

  is minimized.

- $\triangle^* =$ minimum discrepancy

Number Partitioning Problem (NPP)

- Given $S = \{a_1, \ldots, a_n\}$ with $a_j \in \mathbb{Z}_{>0}$, $\alpha = \sum_j a_j$,
- divide S into 2 disjoint subsets $S_1 \cup S_2 = S$ such that

$$\triangle = \left| \sum_{j \in S_1} a_j \; - \; \sum_{j \in S_2} a_j \right|, \text{ the } \textit{discrepancy},$$

  is minimized.

- $\triangle^* =$ minimum discrepancy
- allocate $\beta = 1/2\ \alpha$, or, as close as possible to β, to each subset

Number Partitioning Problem (NPP)

Number Partitioning Problem (NPP)

- one of six basic NP-complete problems in Garey and Johnson (79)

Number Partitioning Problem (NPP)

- one of six basic NP-complete problems in Garey and Johnson (79)
- only one dealing directly with *numbers*

Number Partitioning Problem (NPP)

- one of six basic NP-complete problems in Garey and Johnson (79)
- only one dealing directly with *numbers*
- *balanced* NPP (BalNPP): $|S_1| = |S_2| = n/2$ (for even n)

NPP – Example

- $S = \{6, 4, 7, 8, 5\}$

WASHINGTON STATE UNIVERSITY

NPP – Example

- $S = \{\,6, 4, 7, 8, 5\,\}$
- $S = \{4, 5, 6, 7, 8\}$

NPP – Example

- $S = \{6, 4, 7, 8, 5\}$

- $S = \{4, 5, 6, 7, 8\}$
  - $S_1 = \{4, 5, 7\}$ with subset sum $= 16$,

NPP – Example

- $S = \{ 6, 4, 7, 8, 5 \}$
- $S = \{4, 5, 6, 7, 8\}$
  - $S_1 = \{4, 5, 7\}$ with subset sum $= 16$,
  - $S_2 = \{6, 8\}$ with subset sum $= 14$;

NPP – Example

- $S = \{6, 4, 7, 8, 5\}$
- $S = \{4, 5, 6, 7, 8\}$
  - $S_1 = \{4, 5, 7\}$ with subset sum $= 16$,
  - $S_2 = \{6, 8\}$ with subset sum $= 14$; $\quad \triangle = 2$

NPP – Example

- $S = \{6, 4, 7, 8, 5\}$

- $S = \{4, 5, 6, 7, 8\}$
  - $S_1 = \{4, 5, 7\}$ with subset sum $= 16$,
  - $S_2 = \{6, 8\}$ with subset sum $= 14; \quad \triangle = 2$

- $S = \{4, 5, 6, 7, 8\}$

NPP – Example

- $S = \{6, 4, 7, 8, 5\}$
- $S = \{4, 5, 6, 7, 8\}$
  - $S_1 = \{4, 5, 7\}$ with subset sum $= 16$,
  - $S_2 = \{6, 8\}$ with subset sum $= 14; \quad \triangle = 2$
- $S = \{4, 5, 6, 7, 8\}$
  - $S_1 = \{4, 5, 6\}$ and $S_2 = \{7, 8\}$

NPP – Example

- $S = \{\,6, 4, 7, 8, 5\,\}$
- $S = \{4, 5, 6, 7, 8\}$
  - $S_1 = \{4, 5, 7\}$ with subset sum $= 16$,
  - $S_2 = \{6, 8\}$ with subset sum $= 14$; $\quad \triangle = 2$
- $S = \{4, 5, 6, 7, 8\}$
  - $S_1 = \{4, 5, 6\}$ and $S_2 = \{7, 8\}$
  - both subset sums $= 15$;

NPP – Example

- $S = \{6, 4, 7, 8, 5\}$
- $S = \{4, 5, 6, 7, 8\}$
  - $S_1 = \{4, 5, 7\}$ with subset sum $= 16$,
  - $S_2 = \{6, 8\}$ with subset sum $= 14; \quad \triangle = 2$
- $S = \{4, 5, 6, 7, 8\}$
  - $S_1 = \{4, 5, 6\}$ and $S_2 = \{7, 8\}$
  - both subset sums $= 15; \quad \triangle = \triangle^* = 0$

NPP – Example

- $S = \{\,6, 4, 7, 8, 5\,\}$

- $S = \{4, 5, 6, 7, 8\}$
  - $S_1 = \{4, 5, 7\}$ with subset sum $= 16$,
  - $S_2 = \{6, 8\}$ with subset sum $= 14; \quad \triangle = 2$

- $S = \{4, 5, 6, 7, 8\}$
  - $S_1 = \{4, 5, 6\}$ and $S_2 = \{7, 8\}$
  - both subset sums $= 15; \quad \triangle = \triangle^* = 0$

- $\triangle^* = 0$ (or $\triangle^* = 1$ when α odd) gives a *perfect* partition

Applications of NPP

Applications of NPP

- practical

- theoretical

WASHINGTON STATE UNIVERSITY

Applications of NPP

- practical
  - scheduling jobs on processors
    (NPP into $k \geq 3$ subsets: multiprocessor scheduling problem)
  - VLSI circuit design
  - public key cryptography
- theoretical

Applications of NPP

- practical
  - scheduling jobs on processors
    (NPP into $k \geq 3$ subsets: multiprocessor scheduling problem)
  - VLSI circuit design
  - public key cryptography
- theoretical
  - phase transition (fully characterized mathematically)
  - NP-completeness of other problems involving numbers – bin packing, knapsack etc.

NPP – known results

- $a_j = U[1, R]$ for $R \in \mathbb{Z}_{>0}$

NPP – known results

- $a_j = U[1, R]$ for $R \in \mathbb{Z}_{>0}$
- median and expected $\triangle^*$ (in the limit)

NPP – known results

- $a_j = U[1, R]$ for $R \in \mathbb{Z}_{>0}$
- median and expected $\triangle^*$ (in the limit)
  - $\triangle^* = O(\sqrt{n}\, 2^{-n}\, R)$ for NPP

WASHINGTON STATE UNIVERSITY

NPP – known results

- $a_j = U[1, R]$ for $R \in \mathbb{Z}_{>0}$
- median and expected $\triangle^*$ (in the limit)
  - $\triangle^* = O(\sqrt{n}\, 2^{-n} R)$ for NPP
  - $\triangle^* = O(\;\; n\; 2^{-n} R)$ for BALNPP

NPP – known results

- $a_j = U[1, R]$ for $R \in \mathbb{Z}_{>0}$
- median and expected $\triangle^*$ (in the limit)
  - $\triangle^* = O(\sqrt{n}\, 2^{-n}\, R)$ for NPP
  - $\triangle^* = O(\;\, n\; 2^{-n}\, R)$ for BalNPP
    - Karmarkar, Karp, Lueker, Odlyzko (88): median $\triangle^*$ for NPP
    - Lueker (98): average $\triangle^*$ for NPP
    - Mertens (98): median and average $\triangle^*$ for BalNPP

Phase transition of NPP and BalNPP

Phase transition of NPP and BalNPP

- Prob($\triangle^* = 0/1$) $\to 1$ as $n \to \infty$ for $R < 2^n$

Phase transition of NPP and BalNPP

- Prob($\triangle^* = 0/1$) $\to 1$ as $n \to \infty$ for $R < 2^n$ (easy phase)

Phase transition of NPP and BalNPP

- Prob($\triangle^* = 0/1$) $\to 1$ as $n \to \infty$ for $R < 2^n$ (easy phase)
- Prob($\triangle^* = 0/1$) $\to 0$ as $n \to \infty$ for $R > 2^n$

Phase transition of NPP and BalNPP

- Prob($\triangle^* = 0/1$) $\rightarrow 1$ as $n \rightarrow \infty$ for $R < 2^n$ (easy phase)
- Prob($\triangle^* = 0/1$) $\rightarrow 0$ as $n \rightarrow \infty$ for $R > 2^n$ (hard phase)

Phase transition of NPP and BalNPP

- Prob$(\triangle^* = 0/1) \rightarrow 1$ as $n \rightarrow \infty$ for $R < 2^n$ (easy phase)
- Prob$(\triangle^* = 0/1) \rightarrow 0$ as $n \rightarrow \infty$ for $R > 2^n$ (hard phase)
  - Gent and Walsh (96): empirical evidence
  - Mertens (98): spin glass analogy
  - Borgs, Chayes, and Pittel (01): complete mathematical analysis

Phase transition of NPP and BalNPP

- Prob$(\triangle^* = 0/1) \to 1$ as $n \to \infty$ for $R < 2^n$ (easy phase)
- Prob$(\triangle^* = 0/1) \to 0$ as $n \to \infty$ for $R > 2^n$ (hard phase)
  - Gent and Walsh (96): empirical evidence
  - Mertens (98): spin glass analogy
  - Borgs, Chayes, and Pittel (01): complete mathematical analysis
- $\#$ perfect partitions $\uparrow$ as $R \downarrow$ with $R < 2^n$

Phase transition of NPP and BalNPP

- $\text{Prob}(\triangle^* = 0/1) \to 1$ as $n \to \infty$ for $R < 2^n$ (easy phase)
- $\text{Prob}(\triangle^* = 0/1) \to 0$ as $n \to \infty$ for $R > 2^n$ (hard phase)
  - Gent and Walsh (96): empirical evidence
  - Mertens (98): spin glass analogy
  - Borgs, Chayes, and Pittel (01): complete mathematical analysis
- $\#$ perfect partitions $\uparrow$ as $R \downarrow$ with $R < 2^n$
- minimum partition unique for $R \gg 2^n$

Karmarkar-Karp differencing (KK)

Karmarkar-Karp differencing (KK)

- maintain sorted list of numbers

Karmarkar-Karp differencing (KK)

- maintain sorted list of numbers
- replace two largest numbers by their difference
  (commit to place them in opposite subsets)

Karmarkar-Karp differencing (KK)

- maintain sorted list of numbers
- replace two largest numbers by their difference (commit to place them in opposite subsets)
- Yakir (96): $\triangle_{KK} = O(n^{-0.72 \log n} R)$

WASHINGTON STATE UNIVERSITY

Karmarkar-Karp differencing (KK)

- maintain sorted list of numbers
- replace two largest numbers by their difference (commit to place them in opposite subsets)
- Yakir (96): $\triangle_{KK} = O(n^{-0.72 \log n} R)$
  recall, $\triangle^* = O(\sqrt{n}\, 2^{-n} R)$

Karmarkar-Karp differencing (KK)

- maintain sorted list of numbers
- replace two largest numbers by their difference
  (commit to place them in opposite subsets)
- Yakir (96): $\triangle_{KK} = O(n^{-0.72 \log n} R)$
  recall, $\triangle^* = O(\sqrt{n}\, 2^{-n} R)$
- running time is $O(n \log n)$

Complete KK heuristic

Complete KK heuristic

- Korf (98), Mertens (99)

Complete KK heuristic

- Korf (98), Mertens (99)
- also consider replacing two largest numbers by their *sum*

Complete KK heuristic

- Korf (98), Mertens (99)
- also consider replacing two largest numbers by their *sum*
- improves on KK discrepancy as it continues to run

Complete KK heuristic

- Korf (98), Mertens (99)
- also consider replacing two largest numbers by their *sum*
- improves on KK discrepancy as it continues to run
- effective in practice in the easy phase

Complete KK heuristic

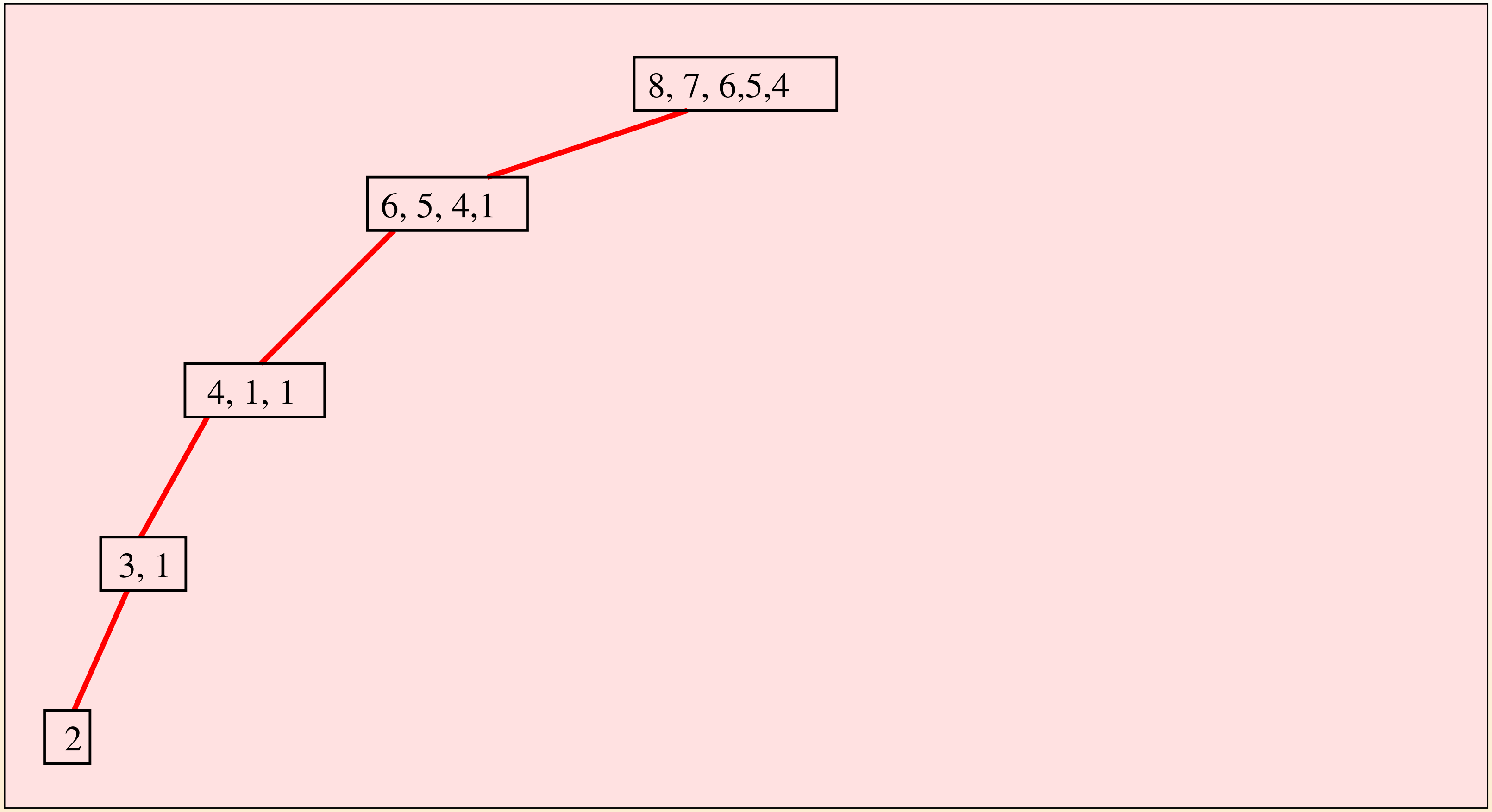
- Korf (98), Mertens (99)
- also consider replacing two largest numbers by their *sum*
- improves on KK discrepancy as it continues to run
- effective in practice in the easy phase
- $\#$ of branch-and-bound nodes is exponential in n when $R > 2^n$

Complete KK heuristic

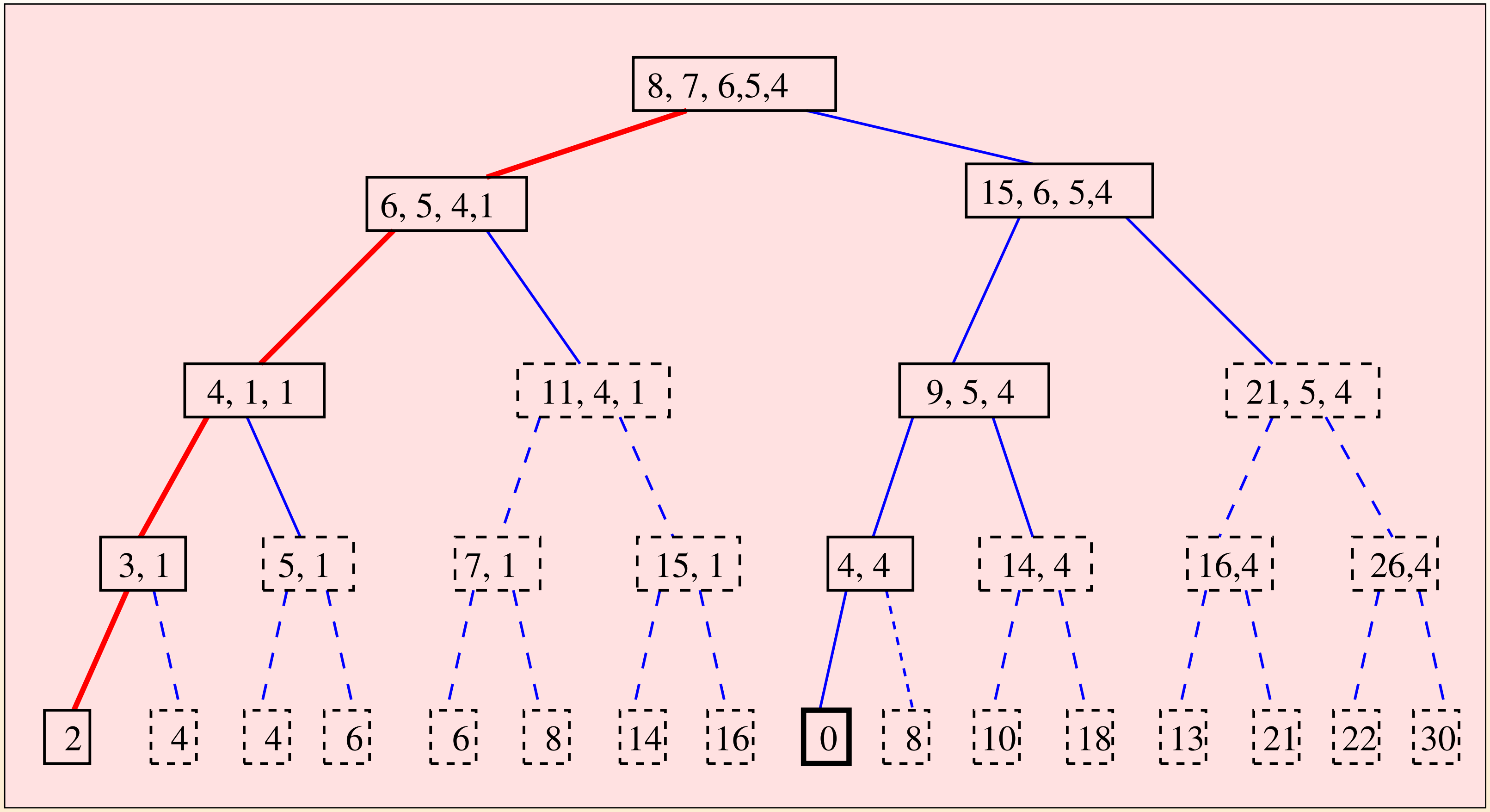
- Korf (98), Mertens (99)
- also consider replacing two largest numbers by their *sum*
- improves on KK discrepancy as it continues to run
- effective in practice in the easy phase
- $\#$ of branch-and-bound nodes is exponential in n when $R > 2^n$
- converges very slowly

KK and CKK: Example

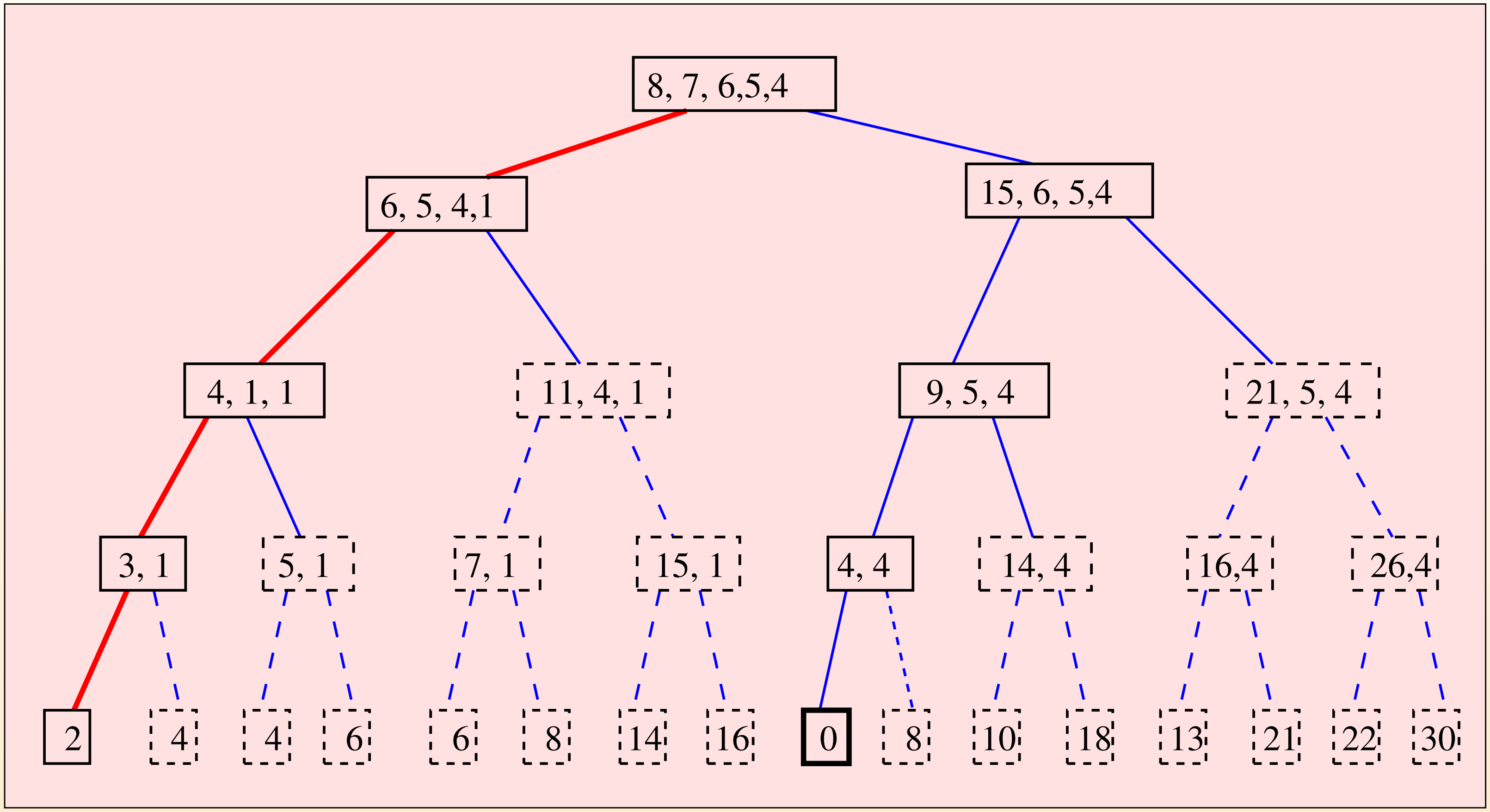
KK and CKK: Example



KK and CKK: Example

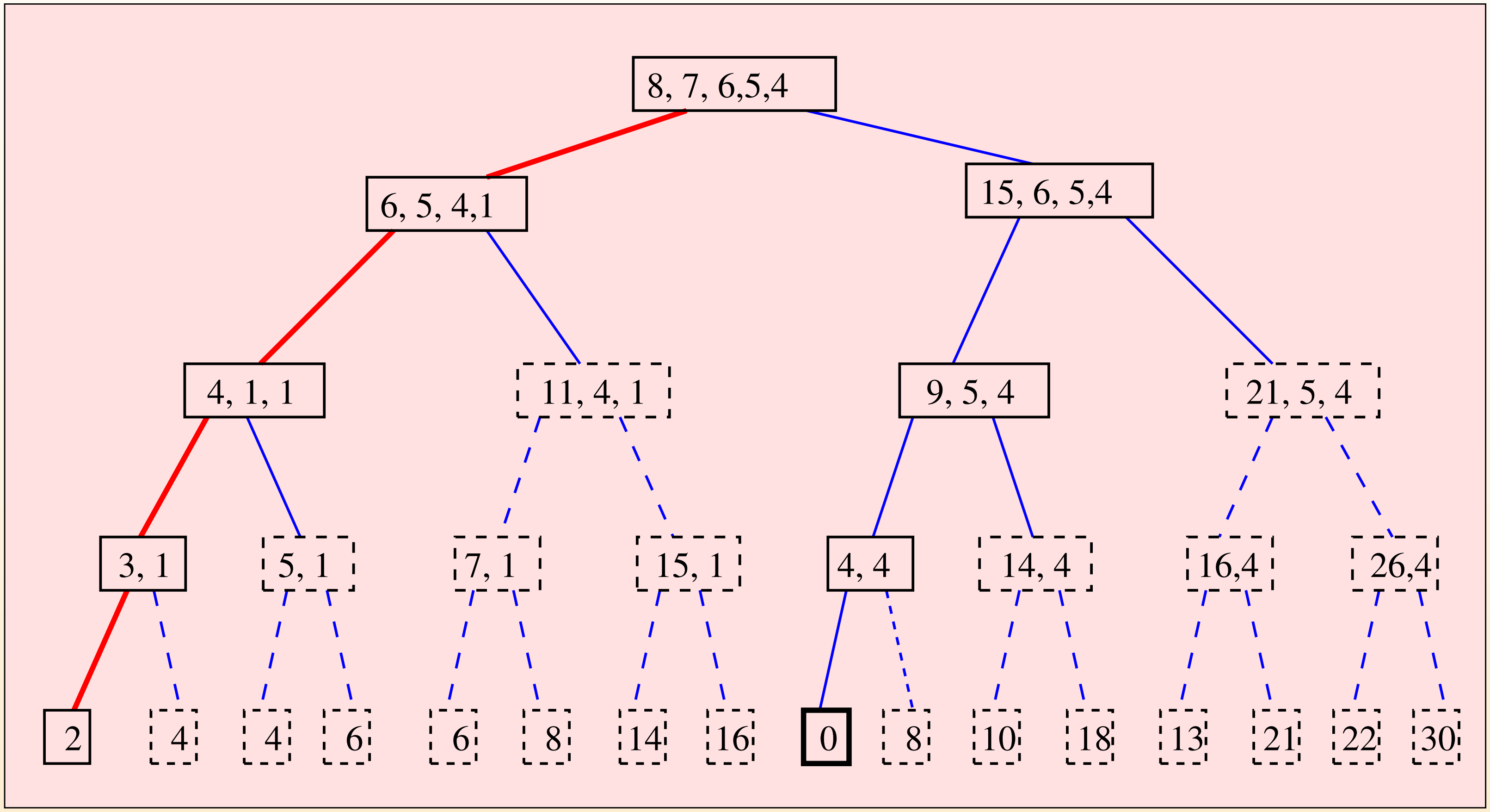


KK and CKK: Example



- dashed parts of the tree are pruned

KK and CKK: Example



- dashed parts of the tree are pruned
- two-color associated tree to recover partition

Algorithms for NPP

Algorithms for NPP

- KK is the *best* polynomial time approx. algo known

Algorithms for NPP

- KK is the *best* polynomial time approx. algo known
- metaheuristics for easy phase (Storer (96))

Algorithms for NPP

- KK is the *best* polynomial time approx. algo known
- metaheuristics for easy phase (Storer (96))
- concentrate on "hard phase" ($R > 2^n$)

Algorithms for NPP

- KK is the *best* polynomial time approx. algo known
- metaheuristics for easy phase (Storer (96))
- concentrate on "hard phase" $(R > 2^n)$
- lattice-based techniques? IP approaches?

Algorithms for NPP

- KK is the *best* polynomial time approx. algo known
- metaheuristics for easy phase (Storer (96))
- concentrate on "hard phase" $(R > 2^n)$
- lattice-based techniques? IP approaches?
- typical numbers are *huge*; for $n = 30$, look at a_j's with 11 digits!

Lattice Problems and NPP

Lattice Problems and NPP

- lattice generated by $\boldsymbol{b_1}, \ldots, \boldsymbol{b_n}$ (LI vectors in $\mathbb{R}^m$) is

Lattice Problems and NPP

- lattice generated by $\boldsymbol{b_1}, \ldots, \boldsymbol{b_n}$ (LI vectors in $\mathbb{R}^m$) is $\mathbb{L} = \left\{ \sum_j \boldsymbol{b_j} x_j \, : \, x_j \in \mathbb{Z} \right\}$.

Lattice Problems and NPP

- lattice generated by $\boldsymbol{b_1}, \ldots, \boldsymbol{b_n}$ (LI vectors in $\mathbb{R}^m$) is $\mathbb{L} = \left\{ \sum_j \boldsymbol{b_j} x_j \, : \, x_j \in \mathbb{Z} \right\}$. $(\boldsymbol{b_1}, \ldots, \boldsymbol{b_n})$ – a basis for $\mathbb{L}$

Lattice Problems and NPP

- lattice generated by $\boldsymbol{b_1}, \ldots, \boldsymbol{b_n}$ (LI vectors in $\mathbb{R}^m$) is $\mathbb{L} = \left\{ \sum_j \boldsymbol{b_j} x_j : x_j \in \mathbb{Z} \right\}$. $(\boldsymbol{b_1}, \ldots, \boldsymbol{b_n})$ – a basis for $\mathbb{L}$

- Closest Vector Problem (decision version - DCVP):

WASHINGTON STATE UNIVERSITY

Lattice Problems and NPP

- lattice generated by $\boldsymbol{b_1}, \ldots, \boldsymbol{b_n}$ (LI vectors in $\mathbb{R}^m$) is $\mathbb{L} = \left\{ \sum_j \boldsymbol{b_j} x_j \, : \, x_j \in \mathbb{Z} \right\}$. $(\boldsymbol{b_1}, \ldots, \boldsymbol{b_n})$ – a basis for $\mathbb{L}$

- Closest Vector Problem (decision version - DCVP):
  Given: lattice basis $B \in \mathbb{Z}^{m \times n}$, target vector $\boldsymbol{u}$, rational $\gamma > 0$,

Lattice Problems and NPP

- lattice generated by $\boldsymbol{b_1}, \ldots, \boldsymbol{b_n}$ (LI vectors in $\mathbb{R}^m$) is $\mathbb{L} = \left\{ \sum_j \boldsymbol{b_j} x_j \, : \, x_j \in \mathbb{Z} \right\}$. $(\boldsymbol{b_1}, \ldots, \boldsymbol{b_n})$ – a basis for $\mathbb{L}$

- Closest Vector Problem (decision version - DCVP):
  Given: lattice basis $B \in \mathbb{Z}^{m \times n}$, target vector $\boldsymbol{u}$, rational $\gamma > 0$,
  find $\boldsymbol{x} \in \mathbb{Z}^n$ s.t. $\| B\boldsymbol{x} - \boldsymbol{u} \| \leq \gamma$, or prove $\| B\boldsymbol{x} - \boldsymbol{u} \| > \gamma \, \forall \, \boldsymbol{x} \in \mathbb{Z}^n$.

Lattice Problems and NPP

- lattice generated by $\boldsymbol{b_1}, \ldots, \boldsymbol{b_n}$ (LI vectors in $\mathbb{R}^m$) is $\mathbb{L} = \left\{\sum_j \boldsymbol{b_j} x_j : x_j \in \mathbb{Z}\right\}$. $(\boldsymbol{b_1}, \ldots, \boldsymbol{b_n})$ – a basis for $\mathbb{L}$

- Closest Vector Problem (decision version - DCVP):
  Given: lattice basis $B \in \mathbb{Z}^{m \times n}$, target vector $\boldsymbol{u}$, rational $\gamma > 0$,
  find $\boldsymbol{x} \in \mathbb{Z}^n$ s.t. $\| B\boldsymbol{x} - \boldsymbol{u} \| \leq \gamma$, or prove $\| B\boldsymbol{x} - \boldsymbol{u} \| > \gamma \, \forall \, \boldsymbol{x} \in \mathbb{Z}^n$.

- Decision version of NPP (DNPP_d): Given numbers $a_1, \ldots, a_n$ and an even number $2d$, decide if a partition exists with $\triangle \leq 2d$.

Lattice Problems and NPP

- lattice generated by $\boldsymbol{b_1}, \ldots, \boldsymbol{b_n}$ (LI vectors in $\mathbb{R}^m$) is $\mathbb{L} = \left\{ \sum_j \boldsymbol{b_j} x_j \,:\, x_j \in \mathbb{Z} \right\}$. $(\boldsymbol{b_1}, \ldots, \boldsymbol{b_n})$ – a basis for $\mathbb{L}$
- Closest Vector Problem (decision version - DCVP): Given: lattice basis $B \in \mathbb{Z}^{m \times n}$, target vector $\boldsymbol{u}$, rational $\gamma > 0$, find $\boldsymbol{x} \in \mathbb{Z}^n$ s.t. $\| B\boldsymbol{x} - \boldsymbol{u} \| \leq \gamma$, or prove $\| B\boldsymbol{x} - \boldsymbol{u} \| > \gamma \, \forall \, \boldsymbol{x} \in \mathbb{Z}^n$.
- Decision version of NPP (DNPP_d): Given numbers $a_1, \ldots, a_n$ and an even number $2d$, decide if a partition exists with $\triangle \leq 2d$. Equivalently, find $\boldsymbol{x} \in \{0,1\}^n$ s.t. $\sum_j a_j x_j = \beta - \delta$ for some $\delta \leq d$, if it exists.

Lattice Problems and NPP

- lattice generated by $\boldsymbol{b_1}, \ldots, \boldsymbol{b_n}$ (LI vectors in $\mathbb{R}^m$) is $\mathbb{L} = \left\{ \sum_j \boldsymbol{b_j} x_j \,:\, x_j \in \mathbb{Z} \right\}$. $(\boldsymbol{b_1}, \ldots, \boldsymbol{b_n})$ – a basis for $\mathbb{L}$
- Closest Vector Problem (decision version - DCVP): Given: lattice basis $B \in \mathbb{Z}^{m \times n}$, target vector $\boldsymbol{u}$, rational $\gamma > 0$, find $\boldsymbol{x} \in \mathbb{Z}^n$ s.t. $\| B\boldsymbol{x} - \boldsymbol{u} \| \leq \gamma$, or prove $\| B\boldsymbol{x} - \boldsymbol{u} \| > \gamma \, \forall \, \boldsymbol{x} \in \mathbb{Z}^n$.
- Decision version of NPP (DNPP_d): Given numbers $a_1, \ldots, a_n$ and an even number $2d$, decide if a partition exists with $\triangle \leq 2d$. Equivalently, find $\boldsymbol{x} \in \{0,1\}^n$ s.t. $\sum_j a_j x_j = \beta - \delta$ for some $\delta \leq d$, if it exists. Here, $\beta = \sum_j a_j / 2$.

Lattice Problems and NPP

- lattice generated by $\boldsymbol{b_1}, \ldots, \boldsymbol{b_n}$ (LI vectors in $\mathbb{R}^m$) is $\mathbb{L} = \left\{ \sum_j \boldsymbol{b_j} x_j : x_j \in \mathbb{Z} \right\}$. $(\boldsymbol{b_1}, \ldots, \boldsymbol{b_n})$ – a basis for $\mathbb{L}$

- Closest Vector Problem (decision version - DCVP): Given: lattice basis $B \in \mathbb{Z}^{m \times n}$, target vector $\boldsymbol{u}$, rational $\gamma > 0$, find $\boldsymbol{x} \in \mathbb{Z}^n$ s.t. $\| B\boldsymbol{x} - \boldsymbol{u} \| \leq \gamma$, or prove $\| B\boldsymbol{x} - \boldsymbol{u} \| > \gamma \, \forall \, \boldsymbol{x} \in \mathbb{Z}^n$.

- Decision version of NPP (DNPP_d): Given numbers $a_1, \ldots, a_n$ and an even number $2d$, decide if a partition exists with $\triangle \leq 2d$. Equivalently, find $\boldsymbol{x} \in \{0,1\}^n$ s.t. $\sum_j a_j x_j = \beta - \delta$ for some $\delta \leq d$, if it exists. Here, $\beta = \sum_j a_j / 2$.

- reduce DNPP to DCVP

DNPP to DCVP

Theorem 1. DNPP_d *is Cook-reducible to* DCVP *for* $d > 0$.

DNPP to DCVP

Theorem 1. DNPP_d *is Cook-reducible to* DCVP *for* $d > 0$.

$$B = \begin{bmatrix} 2d\ I \\ \boldsymbol{a}^T \end{bmatrix},$$

WASHINGTON STATE UNIVERSITY

DNPP to DCVP

Theorem 1. DNPP_d *is Cook-reducible to* DCVP *for* $d > 0$.

$$B = \begin{bmatrix} 2d\, I \\ \boldsymbol{a}^T \end{bmatrix}, \quad \boldsymbol{u} = \begin{bmatrix} d\, \mathbf{1} \\ \beta \end{bmatrix}.$$

DNPP to DCVP

Theorem 1. DNPP_d *is Cook-reducible to* DCVP *for* $d > 0$.

$$B = \begin{bmatrix} 2d\, I \\ \boldsymbol{a}^T \end{bmatrix}, \quad \boldsymbol{u} = \begin{bmatrix} d\, \mathbf{1} \\ \beta \end{bmatrix}.$$

- output of reduction: DCVP instance $(B, \boldsymbol{u}, d\sqrt{n+1})$

DNPP to DCVP

Theorem 1. DNPP_d *is Cook-reducible to* DCVP *for* $d > 0$.

$$B = \begin{bmatrix} 2d\, I \\ \boldsymbol{a}^T \end{bmatrix}, \quad \boldsymbol{u} = \begin{bmatrix} d\, \mathbf{1} \\ \beta \end{bmatrix}.$$

- output of reduction: DCVP instance $(B, \boldsymbol{u}, d\sqrt{n+1})$
- generalization of Micciancio (2001) reduction of subset sum to CVP

DBalNPP to DCVP

DBalNPP to DCVP

- DBalNPP$_d$: Given $a_1, \ldots, a_n$ and an even number $2d > 0$, decide if a balanced partition exists with $\triangle \leq 2d$.

DBalNPP to DCVP

- DBalNPP$_d$: Given $a_1, \ldots, a_n$ and an even number $2d > 0$, decide if a balanced partition exists with $\triangle \leq 2d$. Equivalently, find $\boldsymbol{x} \in \{0,1\}^n$ with $\sum_j x_j = \lfloor n/2 \rfloor$ s.t. $\sum_j a_j x_j = \beta - \delta$ or $\sum_j a_j x_j = \beta + \delta$, for some $\delta \leq d$, if it exists.

$\mathrm{DBalNPP}$ to DCVP

- $\mathrm{DBalNPP}_d$: Given $a_1, \ldots, a_n$ and an even number $2d > 0$, decide if a balanced partition exists with $\triangle \leq 2d$. Equivalently, find $\boldsymbol{x} \in \{0,1\}^n$ with $\sum_j x_j = \lfloor n/2 \rfloor$ s.t. $\sum_j a_j x_j = \beta - \delta$ or $\sum_j a_j x_j = \beta + \delta$, for some $\delta \leq d$, if it exists.

  Theorem 2. $\mathrm{DBalNPP}_d$ *is Cook-reducible to* DCVP *for* $d > 0$.

DBalNPP to DCVP

- DBalNPP_d: Given $a_1, \ldots, a_n$ and an even number $2d > 0$, decide if a balanced partition exists with $\triangle \leq 2d$. Equivalently, find $\boldsymbol{x} \in \{0,1\}^n$ with $\sum_j x_j = \lfloor n/2 \rfloor$ s.t. $\sum_j a_j x_j = \beta - \delta$ or $\sum_j a_j x_j = \beta + \delta$, for some $\delta \leq d$, if it exists.

Theorem 2. *DBalNPP_d is Cook-reducible to DCVP for $d > 0$.*

$$B' = \begin{bmatrix} 2d\, I \\ (d+1)\mathbf{1}^T \\ \boldsymbol{a}^T \end{bmatrix}, \quad \boldsymbol{u'} = \begin{bmatrix} d\,\mathbf{1} \\ (d+1)\lfloor n/2 \rfloor \\ \beta \end{bmatrix}.$$

DBALNPP to DCVP

- DBALNPP_d: Given $a_1, \ldots, a_n$ and an even number $2d > 0$, decide if a balanced partition exists with $\triangle \leq 2d$. Equivalently, find $\boldsymbol{x} \in \{0,1\}^n$ with $\sum_j x_j = \lfloor n/2 \rfloor$ s.t. $\sum_j a_j x_j = \beta - \delta$ or $\sum_j a_j x_j = \beta + \delta$, for some $\delta \leq d$, if it exists.

  Theorem 2. DBALNPP_d *is Cook-reducible to* DCVP *for* $d > 0$.

$$B' = \begin{bmatrix} 2d\, I \\ (d+1)\mathbf{1}^T \\ \boldsymbol{a}^T \end{bmatrix}, \quad \boldsymbol{u'} = \begin{bmatrix} d\,\mathbf{1} \\ (d+1)\lfloor n/2 \rfloor \\ \beta \end{bmatrix}.$$

- output of reduction: DCVP instance $(B', \boldsymbol{u'}, d\sqrt{n+1})$

A lattice algorithm for NPP

WASHINGTON STATE UNIVERSITY

A lattice algorithm for NPP

- Given a DCVP *oracle*, do a binary search on $[0, \beta]$ for $\triangle^*$

Washington State University

A lattice algorithm for NPP

- Given a DCVP *oracle*, do a binary search on $[0, \beta]$ for $\triangle^*$
- NPP is solved using a polynomial $\#$ calls to the oracle

A lattice algorithm for NPP

- Given a DCVP *oracle*, do a binary search on $[0, \beta]$ for $\triangle^*$
- NPP is solved using a polynomial $\#$ calls to the oracle
- **but,**

A lattice algorithm for NPP

- Given a DCVP *oracle*, do a binary search on $[0, \beta]$ for $\triangle^*$
- NPP is solved using a polynomial $\#$ calls to the oracle
- **but,** DCVP is NP-complete!

WASHINGTON STATE UNIVERSITY

A lattice algorithm for NPP

- Given a DCVP *oracle*, do a binary search on $[0, \beta]$ for $\triangle^*$
- NPP is solved using a polynomial $\#$ calls to the oracle
- **but,** DCVP is NP-complete! no such oracle exists for large n

A lattice algorithm for NPP

- Given a DCVP *oracle*, do a binary search on $[0, \beta]$ for $\triangle^*$
- NPP is solved using a polynomial $\#$ calls to the oracle
- **but,** DCVP is NP-complete! no such oracle exists for large n
- algo does not use estimates on expected $\triangle^*$

A Basis Reduction Heuristic for NPP

A Basis Reduction Heuristic for NPP

- (try to) solve DCVP using *basis reduction* (BR) on

A Basis Reduction Heuristic for NPP

- (try to) solve DCVP using *basis reduction* (BR) on

$$D = \begin{bmatrix} B & \boldsymbol{u} \\ \boldsymbol{0} & M \end{bmatrix} = \begin{bmatrix} 2d\, I & d\boldsymbol{1} \\ \boldsymbol{a}^T & \beta \\ \boldsymbol{0} & M \end{bmatrix},$$

A Basis Reduction Heuristic for NPP

- (try to) solve DCVP using *basis reduction* (BR) on

$$D = \begin{bmatrix} B & \boldsymbol{u} \\ \mathbf{0} & M \end{bmatrix} = \begin{bmatrix} 2d\, I & d\mathbf{1} \\ \boldsymbol{a}^T & \beta \\ \mathbf{0} & M \end{bmatrix}, \quad \text{where } M \text{ is a large number.}$$

A Basis Reduction Heuristic for NPP

- (try to) solve DCVP using *basis reduction* (BR) on

$$D = \begin{bmatrix} B & \boldsymbol{u} \\ \boldsymbol{0} & M \end{bmatrix} = \begin{bmatrix} 2d\,I & d\boldsymbol{1} \\ \boldsymbol{a}^T & \beta \\ \boldsymbol{0} & M \end{bmatrix}, \quad \text{where } M \text{ is a large number.}$$

- $\mathrm{DCVP} \rightarrow$ shortest vector problem (SVP); Kannan (87)

A Basis Reduction Heuristic for NPP

- (try to) solve DCVP using *basis reduction* (BR) on

$$D = \begin{bmatrix} B & \boldsymbol{u} \\ \mathbf{0} & M \end{bmatrix} = \begin{bmatrix} 2d\, I & d\mathbf{1} \\ \boldsymbol{a}^T & \beta \\ \mathbf{0} & M \end{bmatrix}, \quad \text{where } M \text{ is a large number.}$$

- DCVP $\rightarrow$ shortest vector problem (SVP); Kannan (87)
- BR: using elementary column operations, produce a basis

A Basis Reduction Heuristic for NPP

- (try to) solve DCVP using *basis reduction* (BR) on

$$D = \begin{bmatrix} B & \boldsymbol{u} \\ \mathbf{0} & M \end{bmatrix} = \begin{bmatrix} 2d\, I & d\mathbf{1} \\ \boldsymbol{a}^T & \beta \\ \mathbf{0} & M \end{bmatrix}, \quad \text{where } M \text{ is a large number.}$$

- $\mathrm{DCVP} \rightarrow$ shortest vector problem (SVP); Kannan (87)
- BR: using elementary column operations, produce a basis whose columns are "short" and "nearly orthogonal"

A Basis Reduction Heuristic for NPP

- (try to) solve DCVP using *basis reduction* (BR) on

$$D = \begin{bmatrix} B & \boldsymbol{u} \\ \mathbf{0} & M \end{bmatrix} = \begin{bmatrix} 2d\, I & d\mathbf{1} \\ \boldsymbol{a}^T & \beta \\ \mathbf{0} & M \end{bmatrix}, \quad \text{where } M \text{ is a large number.}$$

- DCVP $\rightarrow$ shortest vector problem (SVP); Kannan (87)
- BR: using elementary column operations, produce a basis whose columns are "short" and "nearly orthogonal"
- with $\triangle^* = \sqrt{n}\, 2^{-n}\, R$, try $d = c\triangle^*$ for several c's in $[1/n, n]$

A Basis Reduction Heuristic for NPP

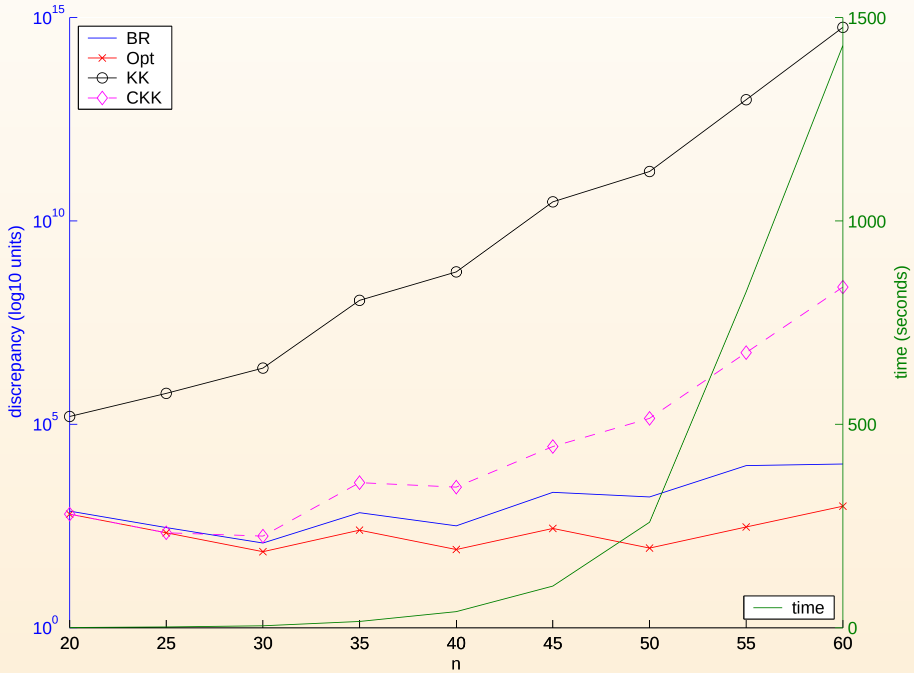
- (try to) solve DCVP using *basis reduction* (BR) on

$$D = \begin{bmatrix} B & \boldsymbol{u} \\ \mathbf{0} & M \end{bmatrix} = \begin{bmatrix} 2d\, I & d\mathbf{1} \\ \boldsymbol{a}^T & \beta \\ \mathbf{0} & M \end{bmatrix}, \quad \text{where } M \text{ is a large number.}$$

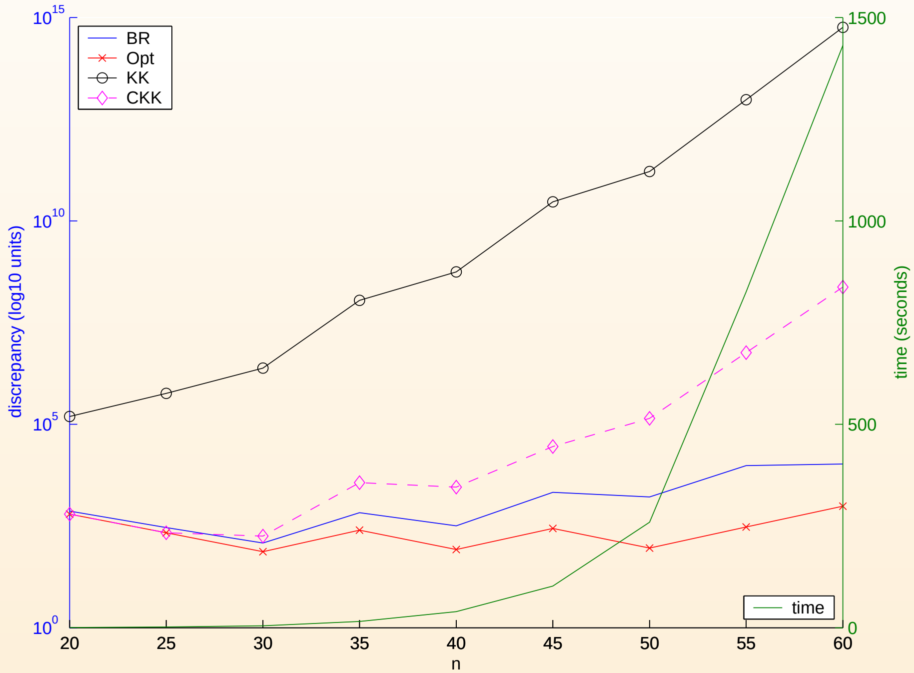
- DCVP $\rightarrow$ shortest vector problem (SVP); Kannan (87)
- BR: using elementary column operations, produce a basis whose columns are “short” and “nearly orthogonal”
- with $\triangle^* = \sqrt{n}\, 2^{-n}\, R$, try $d = c\triangle^*$ for several c's in $[1/n, n]$
- Lagarias & Odlyzko (85), Coster et al. (92): for subset sums

BR Algo Tests:

BR Algo Tests: for NPP

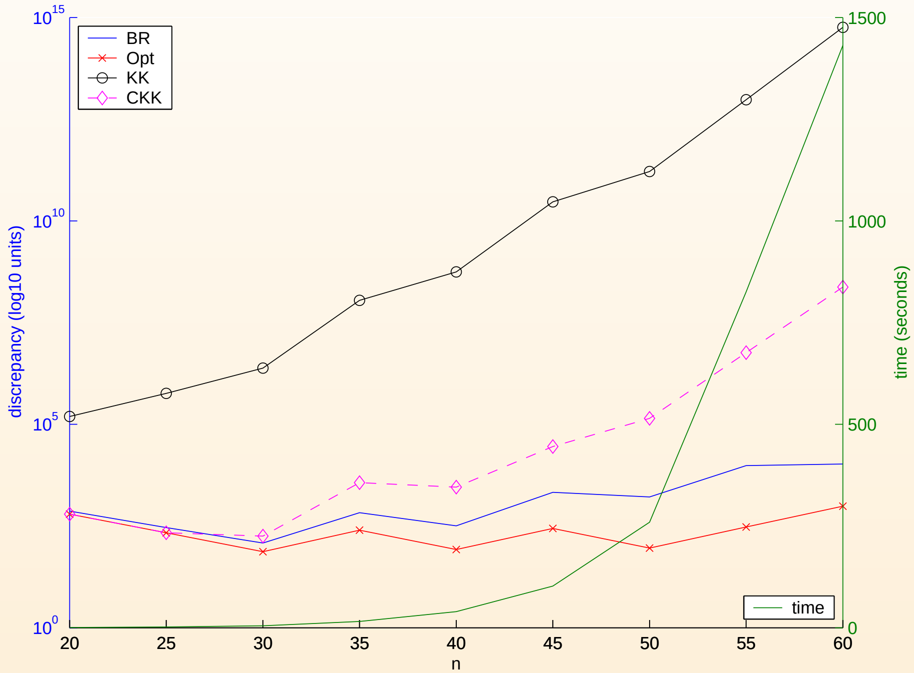


BR Algo Tests: for NPP



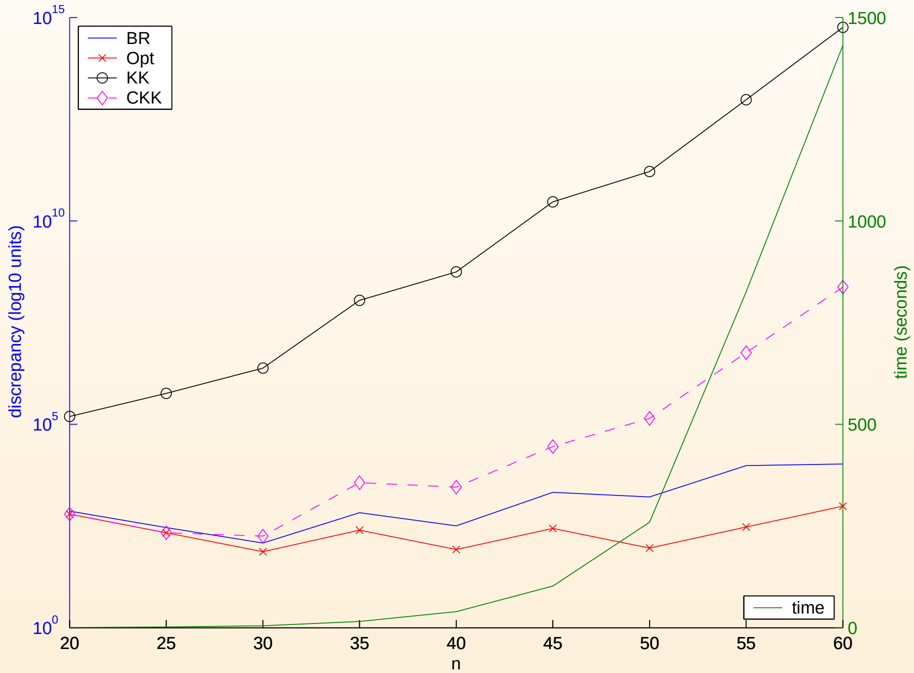
- block Korkine-Zolotarev (BKZ) reduction

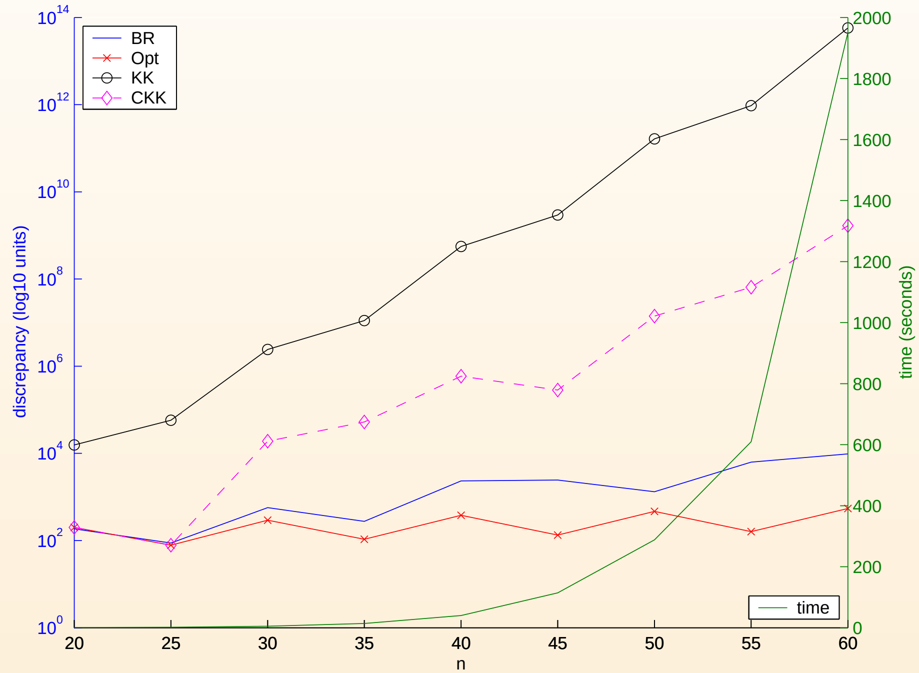
BR Algo Tests: for NPP



- block Korkine-Zolotarev (BKZ) reduction
- opt: $\triangle^* = \sqrt{n}\, 2^{-n}\, R$ is plotted
- ckk: estimated $\triangle_{CKK}$ for same running time as BR

BR Algo Tests: for NPP and BalNPP





- block Korkine-Zolotarev (BKZ) reduction
- opt: $\triangle^* = \sqrt{n}\, 2^{-n}\, R$ is plotted
- ckk: estimated $\triangle_{CKK}$ for same running time as BR

Mixed Integer Program (MIP) for NPP

Mixed Integer Program (MIP) for NPP

- let $x_j = 1$ if a_j is put in first subset, and 0 otherwise; and
  $w =$ deviation from perfect division for first subset.

Mixed Integer Program (MIP) for NPP

- let $x_j = 1$ if a_j is put in first subset, and 0 otherwise; and
  $w =$ deviation from perfect division for first subset.
  Discrepancy $\triangle = 2w$.

Mixed Integer Program (MIP) for NPP

- let $x_j = 1$ if a_j is put in first subset, and 0 otherwise; and
  $w =$ deviation from perfect division for first subset.
  Discrepancy $\triangle = 2w$.

  MIP for NPP:

$$
\begin{array}{llll}
\min & 2w & & \\
\text{s.t.} & w & \geq & \sum a_j x_j - \beta \\
& w & \geq & -\sum a_j x_j + \beta \\
& x_j & \in & \{0,1\} \qquad\qquad j = 1, \ldots, n.
\end{array}
$$

Rangespace Reformulation (RSRef)

Rangespace Reformulation (RSRef)

- write NPP MIP as $\min\{\, w \mid Ax + Bw \leq b,\ x \in \mathbb{Z}^n \,\}$ with

$$A = \begin{bmatrix} \boldsymbol{a}^T \\ -\boldsymbol{a}^T \\ -I \\ I \end{bmatrix}, \quad B = \begin{bmatrix} -1 \\ -1 \\ 0 \\ 0 \end{bmatrix}, \quad \text{and} \quad b = \begin{bmatrix} \beta \\ -\beta \\ 0 \\ 1 \end{bmatrix};$$

WASHINGTON STATE UNIVERSITY

Rangespace Reformulation (RSRef)

- write NPP MIP as $\min\{\, w \,|\, Ax + Bw \leq b,\ x \in \mathbb{Z}^n \,\}$ with

$$A = \begin{bmatrix} \boldsymbol{a}^T \\ -\boldsymbol{a}^T \\ -I \\ I \end{bmatrix},\ B = \begin{bmatrix} -1 \\ -1 \\ 0 \\ 0 \end{bmatrix},\ \text{and}\ \ b = \begin{bmatrix} \beta \\ -\beta \\ 0 \\ 1 \end{bmatrix};$$

apply basis reduction on $D = \begin{bmatrix} A & b \\ 0 & M \end{bmatrix}$ to obtain $\tilde{D} = \begin{bmatrix} \tilde{A} & \tilde{b} \\ 0 & M \end{bmatrix}$,

Rangespace Reformulation (RSRef)

- write NPP MIP as $\min\{\, w \mid Ax + Bw \leq b,\ x \in \mathbb{Z}^n \,\}$ with

$$A = \begin{bmatrix} \boldsymbol{a}^T \\ -\boldsymbol{a}^T \\ -I \\ I \end{bmatrix},\ B = \begin{bmatrix} -1 \\ -1 \\ 0 \\ 0 \end{bmatrix},\ \text{and}\ \ b = \begin{bmatrix} \beta \\ -\beta \\ 0 \\ 1 \end{bmatrix};$$

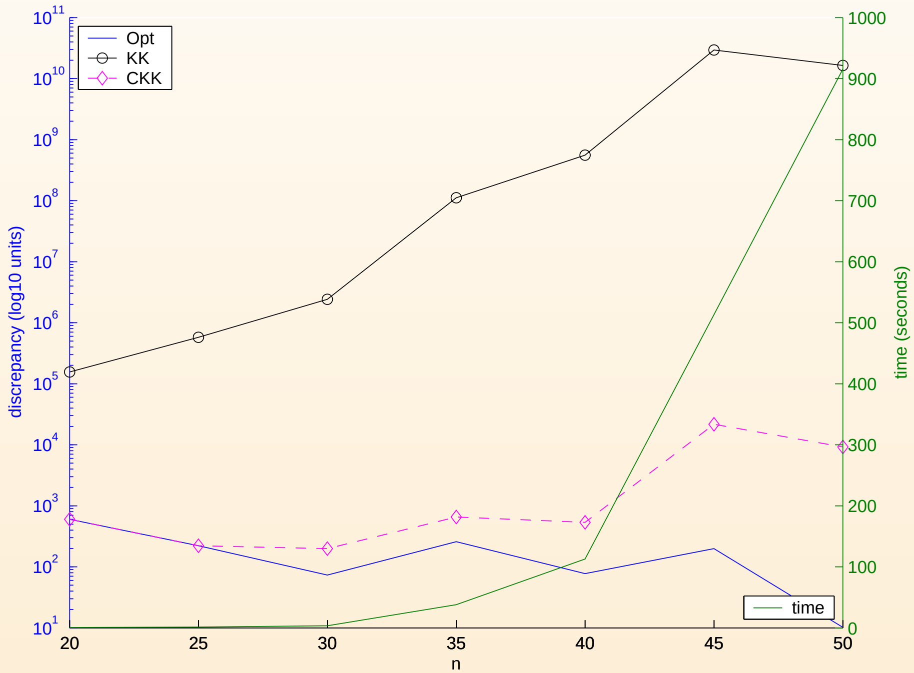
  apply basis reduction on $D = \begin{bmatrix} A & b \\ 0 & M \end{bmatrix}$ to obtain $\tilde{D} = \begin{bmatrix} \tilde{A} & \tilde{b} \\ 0 & M \end{bmatrix}$,

- solve the *rangespace reformulation* using standard solver:

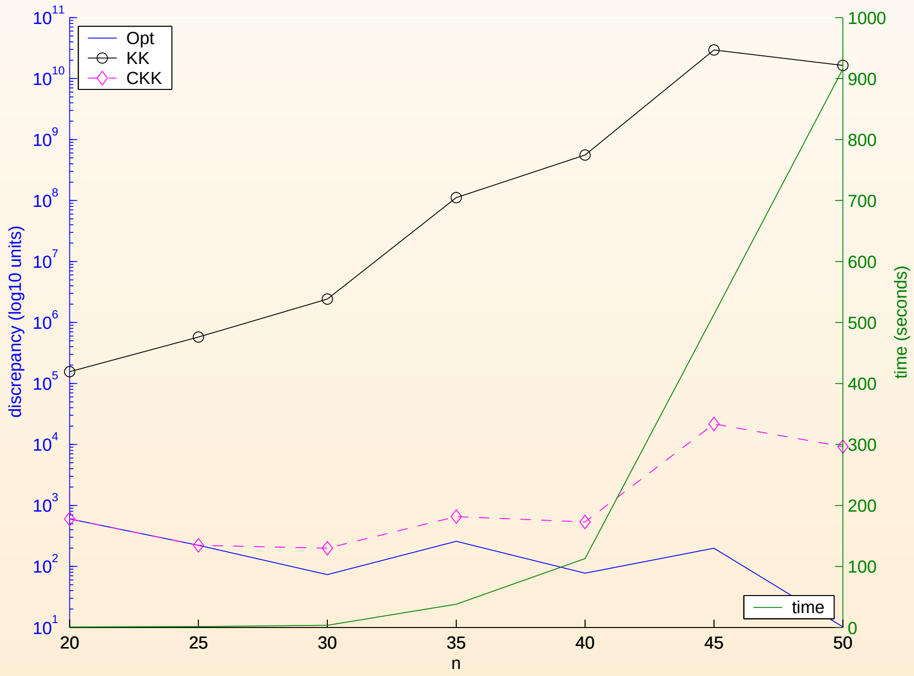
$$\min\{\, w \mid \tilde{A}y + Bw \leq \tilde{b},\ y \in \mathbb{Z}^n \,\}$$

RSRef Tests:

RSRef Tests: on NPP

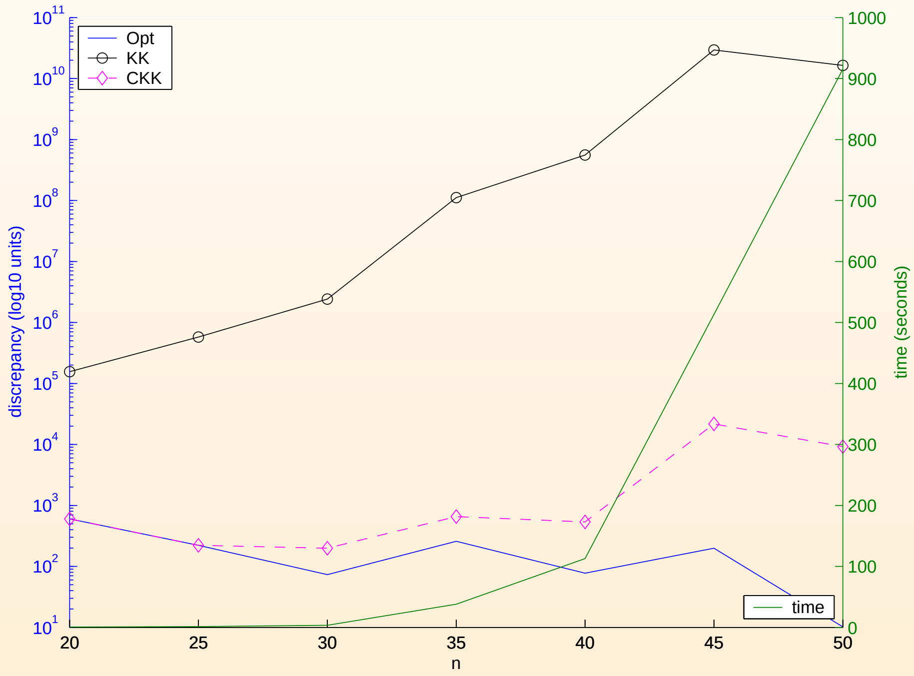


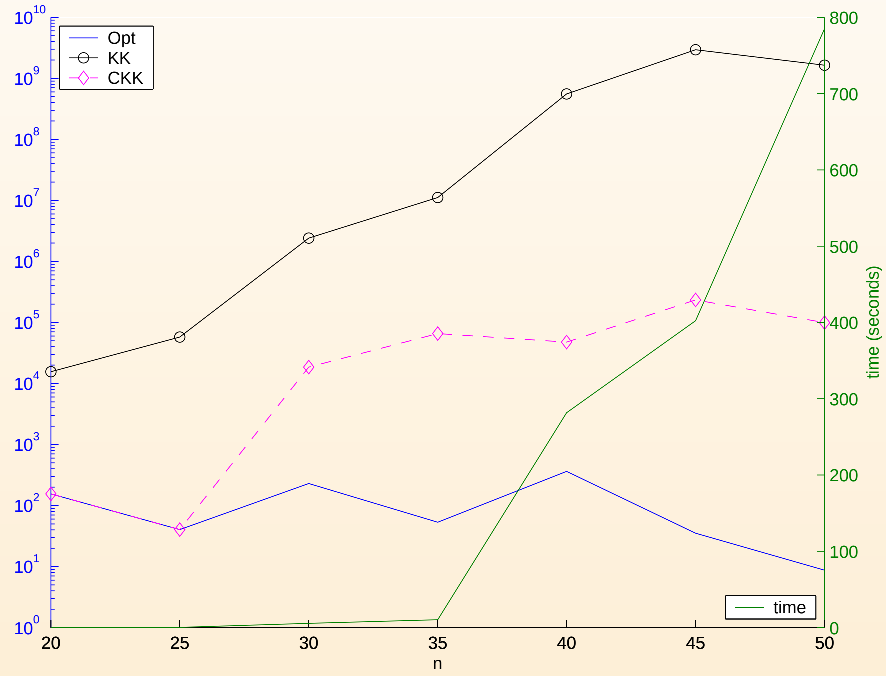
RSRef Tests: on NPP



- BKZ for BR, CPLEX 9.0 as MIP solver

RSRef Tests: on NPP and BalNPP





- BKZ for BR, CPLEX 9.0 as MIP solver

Truncated NPP (TruncNPP)

Truncated NPP (TruncNPP)

- Given the problem $\min\{\,|\sum a_j x_j - \beta|,\ x_j \in \{0,1\}\,\}$,

Truncated NPP (TruncNPP)

- Given the problem $\min\{\,|\sum a_j x_j - \beta|,\ x_j \in \{0,1\}\,\}$, solve

$$\min\{\,|\sum \bar{a}_j x_j - \bar{\beta}|,\ x_j \in \{0,1\}\,\},$$

Truncated NPP (TruncNPP)

- Given the problem $\min\{\,|\sum a_j x_j - \beta|,\; x_j \in \{0,1\}\,\}$, solve

$$\min\{\,|\sum \bar{a}_j x_j - \bar{\beta}|,\; x_j \in \{0,1\}\,\},$$

where $\bar{a}_j = \lfloor a_j/T \rceil$ and $\bar{\beta} = 1/2\ \bar{\alpha}$ with $\bar{\alpha} = \sum \bar{a}_j$.

Truncated NPP (TruncNPP)

- Given the problem $\min\{\,|\sum a_j x_j - \beta|,\; x_j \in \{0,1\}\,\}$, solve

$$\min\{\,|\sum \bar{a}_j x_j - \bar{\beta}|,\; x_j \in \{0,1\}\,\},$$

  where $\bar{a}_j = \lfloor\, a_j/T \,\rceil$ and $\bar{\beta} = 1/2\;\bar{\alpha}$ with $\bar{\alpha} = \sum \bar{a}_j$.

- with $T = 10^t$ for $t \geq 1$, we *truncate* the last t digits from each a_j

Truncated NPP (TruncNPP)

- Given the problem $\min\{\,|\sum a_j x_j - \beta|,\ x_j \in \{0,1\}\,\}$, solve

$$\min\{\,|\sum \bar{a}_j x_j - \bar{\beta}|,\ x_j \in \{0,1\}\,\},$$

where $\bar{a}_j = \lfloor a_j/T \rceil$ and $\bar{\beta} = 1/2\ \bar{\alpha}$ with $\bar{\alpha} = \sum \bar{a}_j$.

- with $T = 10^t$ for $t \geq 1$, we *truncate* the last t digits from each a_j

Theorem 3. *Let $\bar{x}$ be an optimal solution to the truncated NPP.*

Truncated NPP (TruncNPP)

- Given the problem $\min\{\,|\sum a_j x_j - \beta|,\ x_j \in \{0,1\}\,\}$, solve

$$\min\{\,|\sum \bar{a}_j x_j - \bar{\beta}|,\ x_j \in \{0,1\}\,\},$$

where $\bar{a}_j = \lfloor a_j/T \rceil$ and $\bar{\beta} = 1/2\ \bar{\alpha}$ with $\bar{\alpha} = \sum \bar{a}_j$.

- with $T = 10^t$ for $t \geq 1$, we *truncate* the last t digits from each a_j

Theorem 3. *Let $\bar{x}$ be an optimal solution to the truncated NPP.*

$$\triangle_T = \left|\sum a_j \bar{x}_j - \beta\right|$$

Truncated NPP (TruncNPP)

- Given the problem $\min\{\,|\sum a_j x_j - \beta|,\ x_j \in \{0,1\}\,\}$, solve

$$\min\{\,|\sum \bar{a}_j x_j - \bar{\beta}|,\ x_j \in \{0,1\}\,\},$$

where $\bar{a}_j = \lfloor a_j/T \rceil$ and $\bar{\beta} = 1/2\,\bar{\alpha}$ with $\bar{\alpha} = \sum \bar{a}_j$.

- with $T = 10^t$ for $t \geq 1$, we *truncate* the last t digits from each a_j

Theorem 3. *Let $\bar{x}$ be an optimal solution to the truncated NPP.*

$$\triangle_T = \left|\sum a_j \bar{x}_j - \beta\right| \leq \triangle^* + (n/2)\,T, \quad \textit{on average.}$$

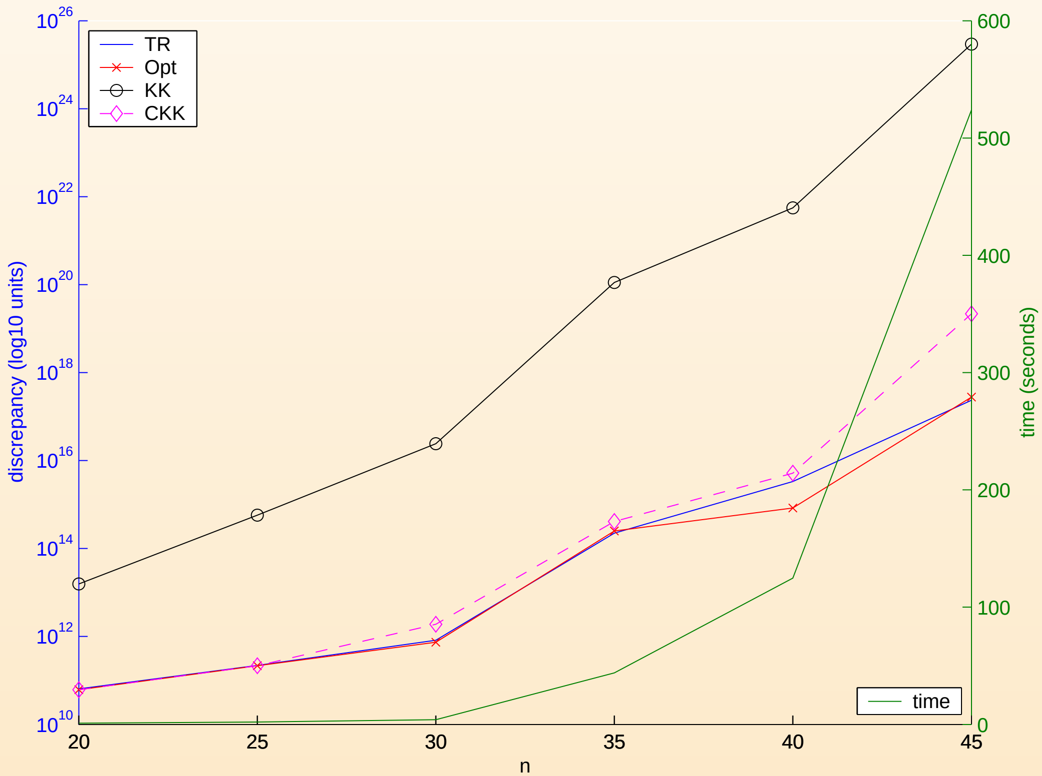
Truncated NPP: Results

Truncated NPP: Results

- solve truncated instances using RSRef (MIP)

Truncated NPP: Results

- solve truncated instances using RSRef (MIP)



Remarks

Remarks

- BR, or even CKK, can be applied to TRUNCNPP

Remarks

- BR, or even CKK, can be applied to TruncNPP
- BR, RSRef, TruncNPP: can be applied to

Remarks

- BR, or even CKK, can be applied to TruncNPP
- BR, RSRef, TruncNPP: can be applied to
  - unequal partitions (e.g., $\beta = 0.3\alpha$)
  - *constrained* partitions ($\sum_j x_j = r \neq n/2$)
  - NPP with $k \geq 3$ subsets, with unequal shares ($\neq 1/k$), and/or cardinality constraints

Remarks

- BR, or even CKK, can be applied to TruncNPP
- BR, RSRef, TruncNPP: can be applied to
  - unequal partitions (e.g., $\beta = 0.3\alpha$)
  - *constrained* partitions ($\sum_j x_j = r \neq n/2$)
  - NPP with $k \geq 3$ subsets, with unequal shares ($\neq 1/k$), and/or cardinality constraints
- lattice algos efficient in practice for reasonably large n

Remarks

- BR, or even CKK, can be applied to $\textsc{TruncNPP}$
- BR, RSRef, $\textsc{TruncNPP}$: can be applied to
  - unequal partitions (e.g., $\beta = 0.3\alpha$)
  - *constrained* partitions ($\sum_j x_j = r \neq n/2$)
  - NPP with $k \geq 3$ subsets, with unequal shares ($\neq 1/k$), and/or cardinality constraints
- lattice algos efficient in practice for reasonably large n
- running times increase with R

Remarks

- BR, or even CKK, can be applied to $\textsc{TruncNPP}$
- BR, RSRef, $\textsc{TruncNPP}$: can be applied to
  - unequal partitions (e.g., $\beta = 0.3\alpha$)
  - *constrained* partitions ($\sum_j x_j = r \neq n/2$)
  - NPP with $k \geq 3$ subsets, with unequal shares ($\neq 1/k$), and/or cardinality constraints
- lattice algos efficient in practice for reasonably large n
- running times increase with R
- for $n \geq 100$, KK may still be the best (current) option

Outline

- Number Partitioning Problem (NPP)
- Karmarkar-Karp differencing (KK)
- NPP and the Closest Vector Problem (CVP)
- A Basis Reduction Heuristic for NPP
- Mixed Integer Program (MIP) for NPP
- Truncated NPP