2013 UKSim 15th International Conference on Computer Modelling and Simulation

An Interesting Cryptography Study Based on Knapsack Problem

Ning Ruan
School of Science, Information Technology and Engineering
University of Ballarat
Ballarat, VIC 3353, Australia
Email: n.ruan@ballarat.edu.au

***Abstract*—Cryptography is an art that has been practised through the centuries. Interest in the applications of the knapsack problem to cryptography has arisen with the advent of public key cryptography. The knapsack problem is well documented problem and all research into its properties have lead to the conjecture that it is difficult to solve. In this paper the canonical duality theory is presented for solving general knapsack problem. By using the canonical dual transformation, the integer programming problem can be converted into a continuous canonical dual problem with zero duality gap. The optimality criterion are also discussed. Numerical examples show the efficiency of the method.**

Keywords-global optimization; integer programming; canonical dual transformation; cryptography; knapsack problems.

I. Primal Problems and Motivation

Cryptography can be regarded as the practice and study of hiding information. The primary goal is to achieve a secure means of transmitting information across and in secure communication channel. Public-key cryptography was invented in 1976 by Whitefield Diffie, Martin Hellman and Ralph Merkle [1]. Public-key cryptography needs two keys. One key tells you how to encrypt (or code) a message and this is public to anyone can use it. The other key allow you to decrypt (or decode) the message. This decryption code is kept kept secret (or private) so only the person who knows the key can decrypt the message. Actually this problem can be transfered to famous knapsack problem [1].

Let's consider the general problem. The quadratic knapsack problem (QKP) [2]–[4] can be defined formally as follows: Assume that n items are given where item i has a positive integer weight w_i. In addition we are given an $n \times n$ nonnegative integer matrix $A = \{a_{ij}\}$, where a_{ii} is the profit achieved if item i is selected and $a_{ij} + a_{ji}$ is a profit achieved if both items i and j are selected for $i < j$. c_i is linear profit coefficient. The (QKP) [5]–[7] calls for selecting an item subset whose overall weight does not exceed a given knapsack capacity d, so as to maximize the overall profit. By introducing a binary variable x_i to indicate whether item i is selected, the problem may be formulated:

$$
\begin{array}{lll}
(\mathcal{P}_{q0}) & \max & P_{q0}(\mathbf{x}) = \frac{1}{2}\mathbf{x}^T A\mathbf{x} + \mathbf{x}^T\mathbf{c} \\
 & \text{s.t.} & \mathbf{w}^T\mathbf{x} \le d, \\
 & & \mathbf{x} \in \{0,1\}^n,
\end{array}
\tag{1}
$$

where $A = A^T \in \mathbb{R}^{n\times n}$ is a general symmetric matrix, $\mathbf{c}$ and $\mathbf{w} \in \mathbb{R}^n$ are given vectors, $d \in \mathbb{R}$ is a given scalar greater than zero. Let $\mathcal{X}_q = \{\mathbf{x} \in \{0,1\}^n | \mathbf{w}^T\mathbf{x} \le d\}$.

Furthermore, if the objective function is lack of quadratic term, the problem simplified to the following:

$$
\begin{array}{lll}
(\mathcal{P}_{l0}) & \max & P_{l0}(\mathbf{x}) = \mathbf{c}^T\mathbf{x} \\
 & \text{s.t.} & \mathbf{w}^T\mathbf{x} \le d, \\
 & & \mathbf{x} \in \{0,1\}^n.
\end{array}
$$

In this paper we presents a generalized canonical duality theory for solving these challenging problems. Canonical duality theory [8] developed from nonconvex analysis and global optimization [9]–[11]. It is a potentially powerful methodology, which has been used successfully for solving a large class of challenging problems in biology [12], network communications [13], and engineering [14]. The rest of the paper is arranged as follows. In section 2, we demonstrate how to rewrite the nonconvex primal problems as a dual problem by using the canonical dual transformation. In section 3, we show that the obtain formulation is canonical dual to the original problems. we illustrate the numerical experiments. The last section presents some conclusions

II. Canonical Dual Transformation for Quadratic Knapsack Problem

we first rewrite the maximization problem to minimization problem.

$$
\begin{array}{lll}
(\mathcal{P}_{qi}) & \min & P_{qi}(\mathbf{x}) = -\frac{1}{2}\mathbf{x}^T A\mathbf{x} - \mathbf{x}^T\mathbf{c} \\
 & \text{s.t.} & \mathbf{w}^T\mathbf{x} \le d, \\
 & & \mathbf{x} \in \{0,1\}^n.
\end{array}
\tag{2}
$$

By the fact that the solution to the quadratic equation $x_i(x_i - 1) = 0$ must be either 0 or 1, the integer constrained problem $(_{\text{II}\rangle})$ can be reformulated to the following quadratic programming problem:

$$
\begin{array}{lll}
(\mathcal{P}_{q}) & \min & P_{q}(\mathbf{x}) = -\frac{1}{2}\mathbf{x}^T A\mathbf{x} - \mathbf{x}^T\mathbf{c} \\
 & \text{s.t.} & \mathbf{w}^T\mathbf{x} \le d, \\
 & & \mathbf{x} \circ (\mathbf{x} - \mathbf{e}) = 0,
\end{array}
\tag{3}
$$

978-0-7695-4994-1/13 $26.00 © 2013 IEEE
DOI 10.1109/UKSim.2013.20

where the notation $\mathbf{s}\circ\mathbf{t} = [s_1t_1, s_2t_2, \cdots, s_nt_n]^T$, denotes the Hadamard product for any two vectors $\mathbf{s}, \mathbf{t} \in \mathbb{R}^n$. $\mathbf{e}$ is an n-dimensional vector with all its entry 1.

In order to apply the canonical duality theory to solve this problem, we need to choose the following geometrically nonlinear operator. Define

$$\begin{aligned}\boldsymbol{\xi} = \Lambda(\mathbf{x}) &= [(\mathbf{w}^T\mathbf{x} \le d)^T, (\mathbf{x}\circ(\mathbf{x}-\mathbf{e}))^T]^T \\ &= [(\boldsymbol{\epsilon})^T, (\boldsymbol{\delta})^T]^T \in \mathbb{R}^{1+n}.\end{aligned}$$

Clearly, this ia a nonlinear mapping. The canonical function associated with this geometrical operator is

$$V(\boldsymbol{\xi}) = \begin{cases} 0 & \text{if } \boldsymbol{\epsilon} \le 0, \boldsymbol{\delta} = 0, \\ +\infty & \text{otherwise.}\end{cases}$$

Let $U(\mathbf{x}) = \frac{1}{2}\mathbf{x}^TA\mathbf{x} + \mathbf{x}^T\mathbf{c}$, originally problem can be rewritten in the canonical form:

$$P(\mathbf{x}) = \mathbf{V}(\Lambda(\mathbf{x})) - U(\mathbf{x}), \mathbf{x} \in \mathbb{R}^n.$$

Define $\boldsymbol{\varsigma} = [(\boldsymbol{\sigma})^T, (\boldsymbol{\mu})^T]^T \in \mathcal{S} = \mathbb{R}^{1+n}$ be the canonical dual variable corresponding to $\boldsymbol{\xi} \in Z = \{(\boldsymbol{\epsilon}, \boldsymbol{\delta}) : \boldsymbol{\epsilon} \le 0, \boldsymbol{\delta} = 0\}$. The couple $(\boldsymbol{\xi}, \boldsymbol{\varsigma})$ forms a canonical duality pair with the Fenchel conjugate of the function $V^\sharp(\boldsymbol{\xi})$ defined by

$$\begin{aligned}V^\sharp(\boldsymbol{\varsigma}) &= \sup\{\boldsymbol{\xi}^T\boldsymbol{\varsigma} - V(\boldsymbol{\xi}) : \boldsymbol{\xi} \in Z\} \\ &= \begin{cases} 0 & \text{if } \boldsymbol{\varsigma} \ge 0, \\ +\infty & \text{otherwise.}\end{cases}\end{aligned}$$

By considering that $V(\boldsymbol{\xi}) = \boldsymbol{\xi}^T\boldsymbol{\varsigma} - \mathbf{V}^\sharp(\boldsymbol{\varsigma})$, the total complementarity function can be defined by

$$\begin{aligned}\Xi(\mathbf{x}, \boldsymbol{\varsigma}) &= \langle \Lambda(\mathbf{x}), \boldsymbol{\varsigma}\rangle - \mathbf{V}^\sharp(\boldsymbol{\varsigma}) - U(\mathbf{x}) \\ &= -\frac{1}{2}\mathbf{x}^TA\mathbf{x} - \mathbf{c}^T\mathbf{x} + \sigma(\mathbf{c}^T\mathbf{x} - \mathbf{d}) \\ &\quad + \boldsymbol{\mu}^T(\mathbf{x}\circ(\mathbf{x}-\mathbf{e})) \\ &= \frac{1}{2}\mathbf{x}^T\mathbf{G}(\boldsymbol{\mu})\mathbf{x} - \mathbf{F}^T(\boldsymbol{\varsigma})\mathbf{x} - \sigma d.\end{aligned}$$

By the criticality condition $\nabla_{\mathbf{x}}\Xi(\mathbf{x}, \boldsymbol{\varsigma}) = 0$, we obtain

$$\mathbf{G}(\boldsymbol{\mu})\mathbf{x} = \mathbf{F}(\boldsymbol{\varsigma}),$$

where

$$\begin{aligned}G(\boldsymbol{\mu}) &= -A + 2\text{Diag }(\boldsymbol{\mu}), \\ F(\sigma, \boldsymbol{\mu}) &= \mathbf{c} - \sigma\mathbf{w} - \sigma d.\end{aligned}$$

Therefore, the canonical dual problem can be formulated as the following.

$$\begin{aligned}(\mathcal{P}_q^d)\ \ \max\ \ & P_q^d(\boldsymbol{\varsigma}) = -\frac{1}{2}\mathbf{F}^T(\sigma, \boldsymbol{\mu})\mathbf{G}^{-1}(\boldsymbol{\mu})\mathbf{F}(\sigma, \boldsymbol{\mu}) \\ & \qquad -\sigma d, \\ \text{s.t.}\ \ & \boldsymbol{\varsigma} \in \mathcal{S}_q,\end{aligned}$$

where dual feasible space is

$$\mathcal{S}_q = \{\boldsymbol{\varsigma} = (\sigma, \boldsymbol{\mu}) \in \mathcal{S} = \mathbb{R}^{1+n} :\ \boldsymbol{\sigma} \ge 0,\ \boldsymbol{\mu} > 0\}.$$

III. Perturbation for Knapsack Problem

Similarly, we rewrite the maximization to minimization problem.

$$\begin{aligned}(\mathcal{P}_{li})\quad \min\quad & P_l(\mathbf{x}) = -\mathbf{c}^T\mathbf{x} \\ \text{s.t.}\quad & \mathbf{w}^T\mathbf{x} \le d, \\ & \mathbf{x} \in \{0, 1\}^n.\end{aligned}$$

Consider knapsack problem do not have quadratic term, one penalty term is added. Let $\mathbf{x} = \frac{1}{2}(\mathbf{y}+\mathbf{e})$, and a be the penalty factor, the knapsack problem can be formulated as

$$\begin{aligned}(\mathcal{P}_l)\quad \min\quad & P_l(\mathbf{y}) = -\frac{1}{2}\mathbf{c}^T(\mathbf{y}+\mathbf{e}) \\ & \quad + \frac{1}{2}a(\mathbf{y}\circ\mathbf{y}-\mathbf{e})^T(\mathbf{y}\circ\mathbf{y}-\mathbf{e}) \\ \text{s.t.}\quad & \mathbf{w}^T(\mathbf{y}+\mathbf{e}) \le 2d, \\ & \mathbf{y}\circ\mathbf{y} - \mathbf{e} = 0.\end{aligned}$$

Let $\mathcal{X}_l = \{\mathbf{y} \in \{0, 1\}^n | \mathbf{w}^T(\mathbf{y}+\mathbf{e}) \le 2d\}$. We choose the geometrically nonlinear operator

$$\boldsymbol{\xi} = \Lambda(\mathbf{y}) = \mathbf{y}\circ\mathbf{y} - \mathbf{e},$$

then, the canonical function associated with this geometrical operator is

$$V(\boldsymbol{\xi}) = \frac{1}{2}a\boldsymbol{\xi}^T\boldsymbol{\xi}.$$

Let $\boldsymbol{\varsigma} \in \mathbb{R}^n$ be the canonical dual variable corresponding to $\boldsymbol{\xi}$,

$$\boldsymbol{\varsigma} = \nabla\mathbf{V}(\boldsymbol{\xi}) = a\boldsymbol{\xi},$$

and the Legendre conjugate of the function $V^\sharp(\boldsymbol{\xi})$ defined by

$$\begin{aligned}V^\sharp(\boldsymbol{\varsigma}) &= \{\boldsymbol{\xi}^T\boldsymbol{\varsigma} - \mathbf{V}(\boldsymbol{\xi}) :\ \boldsymbol{\varsigma} = \nabla\mathbf{V}(\boldsymbol{\xi})\} \\ &= \frac{1}{2}a^{-1}\boldsymbol{\varsigma}^T\boldsymbol{\varsigma}.\end{aligned}$$

Thus, the total complementarity function can be defined by

$$\begin{aligned}\Xi(\mathbf{y}, \boldsymbol{\varsigma}, \sigma, \boldsymbol{\mu}) &= (\mathbf{y}\circ\mathbf{y}-\mathbf{e})^T\boldsymbol{\varsigma} - \frac{1}{2}a^{-1}\boldsymbol{\varsigma}^T\boldsymbol{\varsigma} - \frac{1}{2}\mathbf{c}^T(\mathbf{y}+\mathbf{e}) \\ &\quad + \sigma(\mathbf{w}^T\mathbf{y} - (2d - \mathbf{w}^T\mathbf{e})) + \boldsymbol{\mu}^T(\mathbf{y}\circ\mathbf{y}-\mathbf{e}) \\ &= \frac{1}{2}\mathbf{y}^T(2\text{Diag }(\boldsymbol{\varsigma}+\sigma))\mathbf{y} - (\frac{1}{2}\mathbf{c} - \sigma\mathbf{w})^T\mathbf{y} \\ &\quad -\frac{1}{2}a^{-1}\boldsymbol{\varsigma}^T\boldsymbol{\varsigma} - \mathbf{e}^T(\boldsymbol{\varsigma}+\boldsymbol{\mu}) \\ &\quad -\sigma(2d - \mathbf{w}^T\mathbf{e}) - 1/2\mathbf{c}^T\mathbf{e}.\end{aligned}$$

By the criticality condition $\nabla_{\mathbf{y}}\Xi(\mathbf{x}, \boldsymbol{\varsigma}, \sigma, \boldsymbol{\mu}) = 0$, we obtain

$$\mathbf{y} = \frac{\frac{1}{2}\mathbf{c} - \sigma\mathbf{w}}{2(\boldsymbol{\varsigma}+\boldsymbol{\mu})}.$$

Therefore, the canonical dual function can be formulated as the following.

$$P_l^d(\boldsymbol{\varsigma},\sigma,\boldsymbol{\mu}) = -\frac{1}{4}\frac{(\frac{1}{2}\mathbf{c}-\sigma\mathbf{w})^2}{(\boldsymbol{\varsigma}+\boldsymbol{\mu})} - \frac{1}{2}a^{-1}\boldsymbol{\varsigma}^2 - \mathbf{e}^T(\boldsymbol{\varsigma}+\boldsymbol{\mu})$$
$$-\sigma(2d-\mathbf{w}^T\mathbf{e}) - \frac{1}{2}\mathbf{c}^T\mathbf{e},$$

and the dual feasible space $\mathcal{S}_l$ is defined as

$$\mathcal{S}_l = \{\boldsymbol{\varsigma}\in\mathbb{R}^n, \sigma\in\mathbb{R}, \boldsymbol{\mu}\in\mathbb{R}^n | \ \sigma\geq 0, \boldsymbol{\mu}>0, \boldsymbol{\varsigma}+\boldsymbol{\mu}\neq 0\}.$$

IV. Optimality Criterion

Theorem 1 (Complementary-Dual Principle): The problem $(\mathcal{P}_q^d)$ is canonically dual to the primal problem $(\mathcal{P}_q)$ in the sense that $(\bar{\mathbf{x}},\bar{\sigma},\bar{\boldsymbol{\mu}})$ is a KKT point of $P^d(\bar{\sigma},\bar{\boldsymbol{\mu}})$ over $(\sigma,\boldsymbol{\mu})\in\mathcal{S}_q$ if and only if $\bar{\mathbf{x}}$ is a KKT point of $(\mathcal{P}_q)$, where $\nabla_{\mathbf{x}}\Xi(\mathbf{x},\boldsymbol{\sigma},\boldsymbol{\mu})=0$. Furthermore, the following relation holds.

$$P_q(\bar{\mathbf{x}}) = \Xi(\bar{\mathbf{x}},\bar{\sigma},\bar{\boldsymbol{\mu}}) = P_q^d(\bar{\sigma},\bar{\boldsymbol{\mu}}).$$

Theorem 1 shows that if $\bar{\mathbf{x}}$ is a KKT point of the primal problem $(\mathcal{P}_q$ if and only if the associated $(\bar{\sigma},\bar{\boldsymbol{\mu}})$ is a KKT point of its canonical dual. Furthermore, they have the same optimal function value. Thus, there is no duality gap between the primal problem $(\mathcal{P}_q)$ and its canonical dual $(\mathcal{P}^d)$.

In order to identify the global minimizer of $(\mathcal{P}_q)$, we introduce

$$\mathcal{S}_q^+ = \{(\sigma,\boldsymbol{\mu})\in\mathcal{S}_q \ | \ G(\sigma,\boldsymbol{\mu})\succeq 0\}$$

Then, we have the following theorem.

Theorem 2 (Global Optimality Condition): Suppose that $(\bar{\mathbf{x}},\bar{\sigma},\bar{\boldsymbol{\mu}})$ is a critical point of $P_q^d(\sigma,\boldsymbol{\mu})$ If $(\bar{\sigma},\bar{\boldsymbol{\mu}})\in\mathcal{S}_q^+$, then $(\bar{\sigma},\bar{\boldsymbol{\mu}})$ is a global maximizer of P^d and $\bar{\mathbf{x}}$ is a global minimizer of P on $\mathcal{X}_q$, i.e.,

$$P_q(\bar{\mathbf{x}}) = \min_{\mathbf{x}\in\mathcal{X}_q} P_q(\mathbf{x}) = \max_{(\sigma,\boldsymbol{\mu})\in\mathcal{S}_q^+} P_q^d(\sigma,\boldsymbol{\mu}) = P_q^d(\bar{\sigma},\bar{\boldsymbol{\mu}}).$$

Theorem 2 provides a sufficient condition for a global minimizer of the primal problem $(\mathcal{P}_q)$.

Similarly, we have optimality criterion for knapsack problem with linear objective function.

Theorem 3: The problem $(\mathcal{P}_l^d)$ is canonically dual to the primal problem $(\mathcal{P}_l)$ in the sense that $(\bar{\mathbf{y}},\bar{\boldsymbol{\varsigma}},\bar{\sigma},\bar{\boldsymbol{\mu}})$ is a KKT point of $P^d(\bar{\boldsymbol{\varsigma}},\bar{\sigma},\bar{\boldsymbol{\mu}})$ over $(\varsigma,\sigma,\boldsymbol{\mu})\in\mathcal{S}_q$ if and only if $\bar{\mathbf{y}}$ in $\mathbb{R}^n$ defined by

$$\bar{\mathbf{x}} = \frac{(\frac{1}{2}\mathbf{c}-\bar{\sigma}\mathbf{w})}{2(\bar{\boldsymbol{\varsigma}}+\bar{\boldsymbol{\mu}})} \tag{4}$$

is a KKT point of $(\mathcal{P}_l)$. Furthermore, the following relation holds.

$$P_l(\bar{\mathbf{y}}) = \Xi(\bar{\mathbf{y}},\bar{\boldsymbol{\varsigma}},\bar{\sigma},\bar{\boldsymbol{\mu}}) = P_l^d(\bar{\boldsymbol{\varsigma}},\bar{\sigma},\bar{\boldsymbol{\mu}}).$$

Proof. By introducing a Lagrange multipliers $(\epsilon,\boldsymbol{\xi})\in\mathbb{R}_-\times\mathbb{R}^n_-(\mathbb{R}^n_- := \{\boldsymbol{\epsilon}\in\mathbb{R}| \ \epsilon\leq 0\})$, the Lagrangian $L:\mathcal{S}_l\times\mathbb{R}_-\times\mathbb{R}^n_-\to\mathbb{R}$ associated with the problem $(\mathcal{P}_l^d)$ is

$$L(\boldsymbol{\varsigma},\boldsymbol{\sigma},\boldsymbol{\mu},\epsilon,\boldsymbol{\xi}) = P_l^d(\boldsymbol{\varsigma},\sigma,\boldsymbol{\mu}) - \boldsymbol{\epsilon}\sigma - \boldsymbol{\xi}^T\boldsymbol{\mu}.$$

It is easy to prove that the criticality conditions

$$\nabla_{\boldsymbol{\varsigma}}L(\boldsymbol{\varsigma},\sigma,\boldsymbol{\mu},\epsilon,\boldsymbol{\xi})=0, \ \ \nabla_{\sigma}L(\boldsymbol{\varsigma},\sigma,\boldsymbol{\mu},\epsilon,\boldsymbol{\xi})=0,$$
$$\nabla_{\boldsymbol{\mu}}L(\boldsymbol{\varsigma},\sigma,\boldsymbol{\mu},\epsilon,\boldsymbol{\xi})=0$$

lead to

$$\epsilon = \nabla_{\sigma}P_l^d(\boldsymbol{\varsigma},\sigma,\boldsymbol{\mu}) = \mathbf{w}^T\mathbf{y} - (2d-\mathbf{w}^T\mathbf{e}),$$
$$\boldsymbol{\xi} = \nabla_{\boldsymbol{\mu}}P_l^d(\boldsymbol{\varsigma},\sigma,\boldsymbol{\mu}) = \mathbf{y}\circ\mathbf{y}-\mathbf{e},$$

and the KKT conditions

$$0<\sigma \ \perp \ \epsilon = 0,$$
$$0\leq\boldsymbol{\mu} \ \perp \ \boldsymbol{\xi}\leq 0,$$

where $\mathbf{y} = \frac{(\frac{1}{2}\mathbf{c}-\sigma\mathbf{w})}{2(\boldsymbol{\varsigma}+\boldsymbol{\mu})}$. This shows that if $(\bar{\boldsymbol{\varsigma}},\bar{\boldsymbol{\sigma}},\bar{\boldsymbol{\tau}})$ is a KKT point of the problem $(\mathcal{P}_l^d)$, then $\bar{\mathbf{y}}$ is a KKT point of the primal problem $(\mathcal{P}_l)$.

By using the equations (4), we have

$$\begin{aligned}
&P_l^d(\bar{\boldsymbol{\varsigma}},\bar{\sigma},\bar{\boldsymbol{\mu}})\\
&= -\frac{1}{4}\frac{(\frac{1}{2}\mathbf{c}-\bar{\sigma}\mathbf{w})^2}{(\bar{\boldsymbol{\varsigma}}+\bar{\boldsymbol{\mu}})} - \frac{1}{2}a^{-1}\bar{\boldsymbol{\varsigma}}^2 - \mathbf{e}^T(\bar{\boldsymbol{\varsigma}}+\bar{\boldsymbol{\mu}})\\
&\quad -\bar{\sigma}(2d-\mathbf{w}^T\mathbf{e}) - \frac{1}{2}\mathbf{c}^T\mathbf{e}\\
&= [4\mathbf{y}\circ(\mathbf{y}-\mathbf{e})]\bar{\boldsymbol{\varsigma}} - \frac{1}{2}a^{-1}\bar{\boldsymbol{\varsigma}}^2 + 2\bar{\sigma}(\mathbf{w}^T\mathbf{y}-d)\\
&\quad +4\bar{\boldsymbol{\mu}}^T[\mathbf{y}\circ(\mathbf{y}-\mathbf{e})] - \mathbf{c}^T\mathbf{y}\\
&= \frac{1}{2}a(\bar{\mathbf{y}}\circ\bar{\mathbf{y}}-\mathbf{e})^T(\bar{\mathbf{y}}\circ\bar{\mathbf{y}}-\mathbf{e})\\
&\quad -\frac{1}{2}\mathbf{c}^T\mathbf{y} - \frac{1}{2}\mathbf{c}^T\mathbf{e} + \bar{\boldsymbol{\mu}}(\mathbf{w}^T\mathbf{y}-(2d-\mathbf{w}^T\mathbf{e}))\\
&\quad +\bar{\sigma}(\bar{\mathbf{y}}\circ\bar{\mathbf{y}}-\mathbf{e})\\
&= P_l(\bar{\mathbf{y}})
\end{aligned}$$

This proves the theorem. □

By introducing a useful feasible space

$$\mathcal{S}_l^+ = \{(\boldsymbol{\varsigma},\tau,\boldsymbol{\sigma})^T\in\mathcal{S}_l \ | \ \boldsymbol{\varsigma}+\boldsymbol{\sigma}>0\},$$

we have the following results.

Theorem 4: Suppose that the vector $(\bar{\boldsymbol{\varsigma}},\bar{\sigma},\bar{\boldsymbol{\mu}})$ is a critical point of the canonical dual function $(\mathcal{P}_l^d)$ and

$$\bar{\mathbf{x}} = \frac{(\frac{1}{2}\mathbf{c}-\bar{\sigma}\mathbf{w})}{2(\bar{\boldsymbol{\varsigma}}+\bar{\boldsymbol{\mu}})}.$$

If $(\bar{\boldsymbol{\varsigma}},\bar{\sigma},\bar{\boldsymbol{\mu}})\in\mathcal{S}_a^+$, then $(\bar{\boldsymbol{\varsigma}},\bar{\sigma},\bar{\boldsymbol{\mu}})$ is a global maximizer of P_l^d on $\mathcal{S}_l^+$, the vector $\bar{\mathbf{y}}$ is a global minimizer of P_l on $\mathcal{X}_l$, and

$$P_l(\bar{\mathbf{y}}) = \min_{\mathbf{y}\in\mathcal{X}_l} P_l(\mathbf{y}) = \max_{(\boldsymbol{\varsigma},\sigma,\boldsymbol{\mu})\in\mathcal{S}_l^+} P_l^d(\boldsymbol{\varsigma},\sigma,\boldsymbol{\mu})$$
$$= P_l^d(\bar{\boldsymbol{\varsigma}},\bar{\sigma},\bar{\boldsymbol{\mu}}).$$

Proof. By Theorem 3, we know that vector $(\bar{\boldsymbol{\varsigma}}, \bar{\sigma}, \bar{\boldsymbol{\mu}}) \in \mathcal{S}_l$ is a KKT point of the problem $(\mathcal{P}^d)$ if and only if $\bar{\mathbf{y}} = \frac{(\frac{1}{2}\mathbf{c}-\bar{\sigma}\mathbf{w})}{2(\bar{\boldsymbol{\varsigma}}+\bar{\boldsymbol{\mu}})}$ is a critical point of the problem $(\mathcal{P}_l)$, and

$$P(\bar{\mathbf{y}}) = P^d(\bar{\boldsymbol{\varsigma}}, \bar{\sigma}, \bar{\boldsymbol{\mu}}).$$

By the fact that the canonical dual function $P^d(\boldsymbol{\varsigma}, \sigma, \boldsymbol{\mu})$ is concave on $\mathcal{S}_l^+$, the critical point $(\bar{\boldsymbol{\varsigma}}, \bar{\sigma}, \bar{\boldsymbol{\mu}}) \in \mathcal{S}_l^+$ is a global maximizer of $P^d(\boldsymbol{\varsigma}, \sigma, \boldsymbol{\mu})$ over $\mathcal{S}_l^+$. This proves the statement (5). □

V. Numerical Simulation

All computational results presented in this section are produced by Matlab. And the original problem we considered is $(\mathcal{P}_{li})$.

Example 1. A 4-dimensional knapsack problem

Let $\mathbf{c} = \{16, 54, 18, 52\}, \mathbf{w} = \{13, 10, 9, 10\}, d = 29$. By solving the dual problem, we have

$$\begin{aligned}
\boldsymbol{\varsigma} &= (0.2781, 0.0061, -3.3285, 0.0082),\\
\sigma &= 0.9279,\\
\boldsymbol{\mu} &= (1.7529, 8.8549, 0.6531, 8.3526).
\end{aligned}$$

and $(\boldsymbol{\varsigma}, \sigma, \boldsymbol{\mu}) \in \mathcal{S}_l^+$, By Theorem 4, we know that

$$(x_1, x_2, x_3, x_4) = \{0, 1, 1, 1\}$$

is a global minimizer.

It's easy to verify that

$$P(\bar{\mathbf{x}}) = P^d(\bar{\boldsymbol{\varsigma}}, \bar{\boldsymbol{\sigma}}, \bar{\tau}) = -124.$$

Example 2. A 5-dimensional knapsack problem

Let $\mathbf{c} = \{24, 13, 23, 15, 16\}, \mathbf{w} = \{12, 7, 11, 8, 9\}, d = 26$. By the canonical dual method, we can find out the global minimizer of problem $P_l(\mathbf{x})$ is

$$(x_1, x_2, x_3, x_4, x_5) = \{0, 1, 1, 1, 0\}$$

is a global minimizer with optimal value of -51.

Example 3. High-dimensional knapsack problem

Consider problem $(\mathcal{P}_{li})$ with n = 100,200, 300, 500, 1000. Their coefficients are generated randomly with uniform distribution. For each problem, $c_i \in (1, 50)$, $w_i \in (1, 50)$, for $i = 1, \cdots, n$. The right hand sides of the linear constraints "d" is chosen such that the feasibility of the test problem is satisfied. More specifically, we let $w_i < d < \sum_{i=1}^{d} w_i$.

We then construct the canonical problem of these problems. It is solved by using the interior-point method from the Optimization Toolbox within the Matlab environment. The specifications of the personal notebook computer used are: Window 7 Enterprise, Intel(R), Core(TM)(2.50 GHZ). Table 1 presents the numerical results.

Table I
Numerical results for large scale Knapsack problems

Dimension of the problem	CPU time
100	6.45
200	9.39
300	14.10
500	49.65
1000	182.31

VI. Conclusions

Knapsack problem has been widely used in public key environment The difficulty of the knapsack problem provide a basic for secret and secure communication. Due the its hardness, we consider the problem, we consider the problem from the point of view of duality. By using the canonical dual transformation developed, the integer programming problem can be converted into a continuous canonical dual problem with zero duality gap. The analytical solution is also obtained. Several numerical examples are provided to show the efficiency of the method.

Acknowledgment

Dr. Ning Ruan was supported by a funding from the Australian Government under the Collaborative Research Networks (CRN) program.

References

[1] A. Billionnet and F. Calmels, "Linear programming for the 0-1 quadratic knapsack problem," *Eur. J. Oper. Res.*, vol. 92, pp. 310–325, 1996.

[2] G. Gallo, P. Hammer, and B. Simeone, "Quadratic knapsack problem," *Math. Program.*, vol. 12, pp. 132–149, 1980.

[3] P. Hammer and D. Rader, "Efficient methods for solving quadratic 0-1 knapsack problems," *INFOR*, vol. 35, pp. 170–182, 1997.

[4] C. Helmberg, F. Rendl, and R. Weismantel, "A semidefinite programming approach to the quadratic knapsack problem," *J. Comb. Optim.*, vol. 4, pp. 197–215, 2000.

[5] P. Michelon and L. Veilleux, "Lagrangian methods for the 0-1 quadratic knapsack problem," *Eur. J. Oper. Res.*, vol. 95, pp. 671–682, 1996.

[6] D. J. Rader and W. Woeginer, "The quadratic 0-1 knapsack problem with series-parallel support," *Oper. Res. Lett.*, vol. 30, pp. 159–166, 2002.

[7] H. Wang, G. Kochenberger, and Y. Xu, "A note on optimal solutions to quadratic knapsack problems," *Int. J. Math. Modell. Numer. Optim.*, vol. 1, pp. 344–351, 2010.

[8] D. Gao, *Duality Principles in Nonconvex Systems: Theory, Methods and Applications*. Dordrecht/Boston/London: Kluwer Academic Publishers, 2000.

[9] D. Gao and N. Ruan, "Complete solutions and optimality criteria for nonconvex quadratic-exponential minimization problem," *Math. Meth. Oper. Res.*, vol. 67, pp. 479–491, 2008.

[10] ——, "On the solutions to quadratic minimization problems with box and integer constraints," *J. Global Optim.*, vol. 47, pp. 463–484, 2010.

[11] D. Gao, N. Ruan, and H. Sherali, “Solutions and optimality criteria for nonconvex constrained global optimization problems,” *J. Global Optim.*, vol. 3, pp. 473–497, 2009.

[12] J. Zhang, D. Gao, and J. Yearwood, “A novel canonical dual computational approach for prion agaaaaga amyloid fibril molecular modelling,” *J. Theor. Biol.*, vol. 284, pp. 149–157, 2011.

[13] D. Gao, N. Ruan, and P. Pardalos, *Canonical dual solutions to sum of fourth-order polynomials minimization problems with applications to sensor network localization*, 1st ed., P. Pardalos, V. Boginski, and C. Commander, Eds. Berlin, Germany: Springer-Verlag, 2011.

[14] D. Gao and R. Ogden, “ulti-solutions to nonconvex variational problems with implications for phase transitions and numerical computation,” *Quarterly J. Mech. Appl. Math.*, vol. 61, pp. 497–522, 2008.