ARE ALL INJECTIVE KNAPSACKS PARTLY SOLVABLE AFTER MULTIPLICATION MODULO Q?

Ingemar Ingemarsson

Extended summary

1. Introduction

An integer knapsack is a set of N (positive) integers.

$$K = (k_1, k_2, \ldots, k_n) \tag{1}$$

X is an array of zeroes and ones of the same length as K.

$$X = (x_1, x_2, \ldots, x_N) \tag{2}$$

S is the inner product of K and X.

$$S = \sum_{i=1}^{N} x_i k_i \tag{3}$$

Given S and K it is usually a very difficult problem to find X. In a special case, though, the derivation of X is easy. If (4) is satisfied for all j then X is readily derived from K and S.

$$k_j > \sum_{i=0}^{j-1} k_i \tag{4}$$

If $S \geq k_j$ then $x_j = 1$, subtract k_j from S and repeat the procedure.

Knapsacks which satisfy (4) are here called solvable. Solvable knapsacks are used by Merkle and Hellman [1] in a public key cryptosystem.

We are interested in a larger class of knapsacks with the following definition.

Definition:

A partly solvable knapsack satisfies (5) for at least one index j.

$$k_j > \sum_{i \neq j} k_i \qquad (5)$$

If K is partly solvable we can obviously find s_j from S and K in (3).

Tore Herlestam [2] has proposed an iterative method to possibly solve for X in (3). Even if K is not partly solvable we might obtain a partly solvable knapsack by multiplication of K with a suitable integer modulo q. We may thus find s_j for some index j. The knapsack is reduced by removing $x_j k_j$ and the procedure is repeated.

Not all knapsacks, however, are transformed into partly solvable knapsacks by multiplication mod q. We are interested in classes of knapsacks which are not partly solvable after multiplication mod q. We also state the hypothesis that if (3) invokes an injective mapping from $\{x_i\}_{i=1}^{N}$ to {S} then the knapsack is partly solvable after multiplication mod q.

2. Multiplicatively transformed knapsacks

We regard transformations of knapsacks of the following type:

$$K \rightarrow bK \bmod q \qquad (6)$$

We rewrite (6):

$$K \rightarrow q\left(\frac{b}{q} K \bmod 1\right) \tag{7}$$

Thus by studying non-integer (real) knapsacks of the form (8) for $C \in (0,1)$ we have covered all transformed knapsacks according to (6).

$$R(c) = cK \bmod 1 \tag{8}$$

We define the function Δ_j:

$$\Delta_j(c) \equiv 2(ck_j \bmod 1) - \sum_{i=1}^{N} (ck_i \bmod 1) \tag{9}$$

By (5) the knapsack R(c) is partly solvable if and only if $\Delta_j(c)$ is positive for some index j.

(Here we have extended the definition of partly solvable knapsacks to non-integer knapsacks.)

The derivate of $\Delta_j(c)$ is not positive for any j (where $\Delta_j(c)$ is continuous) if K is not partly solvable. Thus for knapsacks K which are not partly solvable we have the following rule:

If $\Delta_j(c)$ is positive for any value $c = c_+$ then it is positive for $c \leq c_+$ down to the nearest discontinuity point.

Thus be searching through all the discontinuity points and testing $\Delta_j(c)$ for all integers j we are certain to discover if K is transformed into a partly solvable knapsack by any transformation of type (6). (Here we have assumed that K is not partly solvable.)

The following theorems are proved in [3]:

Theorem 1

If K is not partly solvable and bK mod q is partly solvable then mK mod k_i is partly solvable for:

$$\frac{m}{k_i} \leq \frac{b}{q} \tag{10}$$

where m and k_i are chosen so that the difference:

$$\delta = \frac{b}{q} - \frac{m}{k_i} \tag{11}$$

is as small as possible.

Corollary 1

If K is not partly solvable and mK mod k_i is not partly solvable for any m and i then bK mod q is not partly solvable for any choice of b and q.

Theorem 1 has a converse:

Theorem 2

If K is not partly solvable and mK mod k_i is partly solvable the bK mod q is partly solvable for some b and some prime q satisfying (10).

3. Knapsacks which are not multiplicatively transformed into partly solvable knapsacks

We are interested in the class of knapsacks which can not be transformed into partly solvable knapsacks by the transformation (6). This is equivalent to saying that $\Delta_j(c)$ is less than or equal to zero for all c and all j.

We have found the following classes of knapsacks which can not be transformed by (6) into partly solvable knapsacks. (See [3] for details.)

$K = (a,a,ab,abc,abcd,\ldots)$

for any positive integers a,b,c,d,...

$K = (a,2a,3a,4a,\ldots)$

for any positive integer a

$$K = (a_1,a_2,\ldots,a_r, \sum_{i=1}^{r} a_i, 2a_1, 2a_2, \ldots, 2a_r)$$

for any positive integers $a_1,\ldots a_r$.

None of the knapsacks above invokes an injective mapping by (3) which supports the hypothesis stated in the introduction.

References

[1] R.C. Merkle and M.E. Hellman: "Hiding information and signatures in trapdoor knapsacks", IEEE Trans. on Inform. Theory, Vol. IT-24, pp. 525-530, September 1978.

[2] T. Herlestam: "Critical Remarks on Some Public-Key Cryptosystems", BIT, Vol. 18 (1978), pp. 493-496.

[3] I. Ingemarsson: "Knapsacks which are not partly solvable after multiplication modulo q. Report RC8515, IBM Thomas J. Watson Research Center.