Electronic Preprint for Journal of Information Processing Vol.21 No.3

Regular Paper

NP-completeness of Arithmetical Restorations

Tomomi Matsui[1,a)]

Received: July 30, 2012, Accepted: January 11, 2013

Abstract: This paper deals with a variation of crypt-arithmetics, called "arithmetical restorations." Arithmetical restorations are problems dealing with the reconstruction of arithmetical sums from which various digits have been erased. We show the NP-completeness of a problem deciding whether a given instance of arithmetical restorations of multiplication sums has a solution or not.

Keywords: crypt-arithmetic, word crypt-arithmetics, alphametics, NP-complete

1. Introduction

Crypt-arithmetic is a type of mathematical puzzle in which the digits of arithmetical sums are replaced by symbols. The objective of the puzzle is to break a code used. That is, to replace each symbol of the crypt-arithmetics by a numeral so that the resulting mathematical expression becomes true. In a typical case, called *alphametic puzzle*, digits are replaced by letters of the alphabet and there is a one-to-one correspondence between the numbers and the letters replacing them. That is, the same digit is always represented by the same letter or symbol. Eppstein [1] showed that the problem of determining if an alphametic puzzle has a solution is NP-complete, when generalized to arbitrary bases. It is easy to see that when we fix the numeral base, there exists a naive linear time algorithm.

This paper deals with a variation of crypt-arithmetics, called "*arithmetical restorations*." Arithmetical restorations are problems dealing with the reconstruction of arithmetical sums from which various digits have been erased. We show the NP-completeness of a problem deciding whether a given instance of arithmetical restorations of multiplication sums has a solution or not. The problem remains NP-complete even if we fix the numerical base to $r \geq 3$. Our proof also gives ASP-completeness of the problem.

2. Arithmetical Restorations

In this paper, we set the numerical base to 10, unless specifically stated. We deal with arithmetical restorations of multiplication sums in which most of the digits have been replaced by asterisks. Each missing digit may be $1, 2, 3, \ldots, 9$ or 0. When the number of digits of a row is greater than 1, the first digit is not equal to 0. **Figure 1** gives an example of arithmetical restorations and its answer.

1 Department of Information and System Engineering, Chuo University, Bunkyo, Tokyo 112–8551, Japan
a) matsui@ise.chuo-u.ac.jp

3. NP-completeness

Given a problem of arithmetical restorations and a solution to the problem, it is not hard to see that we can verify the solution quickly. Thus, arithmetical restorations are in NP and it remains to show that they are complete for NP.

First, we introduce *Monotone One-in-Three 3SAT*, which is a well-known NP-complete problem.

Monotone One-in-Three 3SAT (e.g., see Ref. [2])

Input: A $p \times q$ matrix A such that (i) each entry is 0 or 1, and (ii) every row contains exactly three 1s.

Question: Is there a vector $z \in \{0, 1\}^q$ satisfying $Az = \mathbf{1}_p$? (The vector $\mathbf{1}_p$ denotes the p-dimensional all one vector.)

Given an instance, a $p \times q$ matrix A, of Monotone One-in-Three 3SAT, we construct an instance of arithmetical restorations for multiplication sums whose first and second rows represent numbers with $1 + pq(q + 1)$ digits and $p(q + 1)(q - 1) + 1$ digits, respectively. We describe a procedure to construct rows of an instance of arithmetical restorations. **Figure 2** gives an example of the following procedure. Each row of an instance of arithmetical restorations is a number. In the following, we denote the number by a vector whose entries are digits of the number.

1st row: We construct the first row in 2 steps as follows. First, we construct a $(1 + pq)$-dimensional row vector $(1, \boldsymbol{a}_1^\top, \boldsymbol{a}_2^\top, \ldots, \boldsymbol{a}_q^\top)$ where $\boldsymbol{a}_j$ is the j-th column vector of a given matrix A. Next, we insert a q-dimensional zero-vector $\mathbf{0}_q^\top$ (indicated by underlines in the first row of Fig. 2) for each pair of consecutive elements of the above vector and obtain a $(1 + pq(q + 1))$-dimensional vector.

2nd row: The second row is obtained from a q-dimensional all-

					*	*	*
×)				*	*	7	*
				*	*	*	*
				*	*	*	
					0		
		*	*	*			
	*	*	*	*	0	*	*

(a) Problem.

					1	4	2
×)				7	0	7	8
				1	1	3	6
				9	9	4	
					0		
		9	9	4			
	1	0	0	5	0	7	6

(b) Answer.

Fig. 1 Arithmetical restorations.

$$\text{Given instance of Monotone One-in-Three 3SAT} \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \begin{bmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}.$$

```
                                                   1 000010000100000 000010000100001 000010000000001 000000000100001
×)                                                   * 00000000000000* 00000000000000* 00000000000000*
------------------------------------------------------------------------------------------------------------------
                                                   * ************** ************** ************** **************
                                                                                                               0
                                                                                                              0
                                                                                                             0
                                                                                                        ...
                                                                                                   0
                                      * ************** ************** ************** **************
                                                                                                  0
                                                                                                 0
                                                                                                0
                                                                                           ...
                                                                                      0
                       * ************** ************** ************** **************
                                                                                     0
                                                                                    0
                                                                                   0
                                                                              ...
                                                                         0
          * *...* ************** ************** **************
------------------------------------------------------------------------------------------------------------------
          * *...* ************** ************** 000040000400004 ************** ************** **************
```

Fig. 2 Reduction to arithmetical restorations.

asterisk row vector by inserting a $(p(q+1)-1)$-dimensional zero-vector $\mathbf{0}^{\top}_{p(q+1)-1}$ for each pair of consecutive asterisks.

3rd, 4th, ..., and $(p(q+1)(q-1)+3)$-th rows: For each $i \in \{3, 4, \ldots, p(q+1)(q-1)+3\}$, we set the i-th row to a $(1+pq(q+1))$-dimensional all-asterisk row vector, if $i = 3 \pmod{p(q+1)}$; and we set the i-th row to 0, otherwise.

bottom row: First, we construct a p-dimensional all-four row vector $4\mathbf{1}^{\top}_{p}$ and insert a q-dimensional zero vector $\mathbf{0}^{\top}_{q}$ for each consecutive pair of elements in $4\mathbf{1}^{\top}_{p}$. Next, we put $((p-1)(q+1)+1)$-dimensional all-asterisk row vector and a $(p-1)(q+1)$-dimensional all-asterisk row vector at the head and the tail of the above vector, respectively.

Consider a case that the arithmetical reconstruction puzzle defined above has a solution. In this paper, a *carry* at the j-th column means an operation of shifting digits into the $(j+1)$-th column when the sum of i-th column exceeds the numerical base. We discuss a carry at the j-th column in the solution where $j = 1 \pmod{p+1}$; e.g., a column corresponding to a digit in the bottom row with underline in Fig. 2. The definition of the above procedure implies that the j-th column in the multiplication sums does not receive a carry from the previous column, if $j = 1 \pmod{p+1}$. We denote the second row of the solution by $(\widetilde{z_1}\mathbf{0}_q\widetilde{z_2}\mathbf{0}_q \cdots \mathbf{0}_q\widetilde{z_q})$. From the definition of the 3rd, 4th, ... rows (except the bottom row), each element in the vector $\widetilde{z} = (\widetilde{z_1}, \widetilde{z_2}, \ldots, \widetilde{z_q})^{\top}$ is a positive integer. Since each row of the matrix A contains exactly three 1s, it is obvious that $\widetilde{z_j} \in \{1, 2\}$ $(j \in \{1, 2, \ldots, q\})$. The definition of the bottom row implies that $A\widetilde{z} = 4\mathbf{1}_p$ and thus $A(\widetilde{z} - \mathbf{1}_q) = \mathbf{1}_p$ and $(\widetilde{z} - \mathbf{1}_q) \in \{0, 1\}^q$ holds. Thus, a given instance of Monotone One-in-Three 3SAT has a solution "YES."

Next, we consider the inverse implication that a given instance of Monotone One-in-Three 3SAT has a solution "YES." We can transform a 0-1 solution of the system of equalities $Az = \mathbf{1}_p$ in a way similar to the above procedure, to the second row of the obtained instance of arithmetical restorations.

From the above discussion, arithmetical restorations are proven to be NP-complete.

4. Discussions

Here we discuss problems of arithmetical restorations defined on a numerical base $r \geq 3$. If $r \geq 5$, a proof appearing in the previous section remains correct.

When $r = 3$ or 4, we only need to replace the subsequence $(\mathbf{0}_q 4\mathbf{0}_q 4 \cdots \mathbf{0}_q 4)$ in the bottom row by

$$(\mathbf{0}_{q-1}10\mathbf{0}_{q-1}10 \cdots \mathbf{0}_{q-1}10) \quad (\text{if } r = 4),$$
$$(\mathbf{0}_{q-1}11\mathbf{0}_{q-1}11 \cdots \mathbf{0}_{q-1}11) \quad (\text{if } r = 3).$$

The NP-completeness of a binary case remains open.

For many sorts of puzzles, the uniqueness of a solution is desired, and thus puzzle designers have to check the uniqueness [3]. This work is exactly an instance of ASP (Another Solution Problem) introduced by Ueda and Nagao [4]. Yato and Seta [6] proved that One-in-Three 3SAT is ASP-complete, where ASP-completeness implies that given a solution to a problem, it is NP-complete to decide if another solution exists. We give a brief proof of the ASP-completeness of Monotone One-in-Three 3SAT in the appendix section. Since our reduction procedure described in the previous section gives a bijection between solution sets of Monotone One-in-Three 3SAT and arithmetical restorations, we have also shown that arithmetical restorations are ASP-complete.

When we solve problems created by puzzle designers, we can assume that a given instance has a unique solution. The assumption offers a possibility that there exists an algorithm which solves every instance with a unique solution in polynomial time. This concept is related to class UP discussed by Valiant in Ref. [5]. UP is the class of sets recognized by nondeterministic polynomial-time Turing machines that for all inputs have either zero or one solution. The influence of the uniquness asumption on arithmetical restorations remains open.

References

[1] Eppstein, D.: On the NP-completeness of cryptarithms, *SIGACT News*, Vol.18, No.3, pp.38–40 (1987).
[2] Garey, M.R. and Johnson, D.S.: *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W.H. Freeman (1979).
[3] Hearn, R.A. and Demaine, E.D.: *Games, Puzzles, and Computation*, A K Peters/CRC Press (2009).
[4] Ueda, N. and Nagao, T.: NP-completeness results for NONOGRAM via parsimonious reductions, Technical Report TR96-0008, Department of Computer Science, Tokyo Institute of Technology (1996).
[5] Valiant, L.G.: Relative complexity of checking and evaluating, *Inf. Process. Lett.*, Vol.5, pp.20–23 (1976).
[6] Yato, T. and Seta, T.: Complexity and completeness of finding another solution and its application to puzzles, *IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences*, Vol.E86-A, No.5, pp.1052–1060 (2003).

Appendix

A.1 ASP-completeness of Monotone One-in-Three 3SAT

In this section, we show the ASP-completeness of Monotone One-in-Three 3SAT. We need to prove that the following problem is NP-complete.

Input: A $p' \times q'$ matrix A' satisfying
(i) each entry is 0 or 1, and
(ii) every row contains exactly three 1s,
and a vector $\boldsymbol{w}^* \in \{0,1\}^{q'}$ satisfying $A'\boldsymbol{w}^* = \mathbf{1}_{p'}$
Question: Is there a 0-1 vector $\boldsymbol{w}' \in \{0,1\}^{q'}$ satisfying both $\boldsymbol{w}' \neq \boldsymbol{w}^*$ and $A'\boldsymbol{w}' = \mathbf{1}_{p'}$?

Given an instance, a $p \times q$ matrix A, of Monotone One-in-Three 3SAT, we construct an instance of the above problem satisfying $p' = 3p + 3$ and $q' = q + 2p + 5$. First, we introduce a small system of equalities;

$$\begin{aligned} v_0 + v_1 + v_2 &= 1, \\ v_0 + v_1 + v_3 &= 1, \\ v_0 + v_2 + v_3 &= 1, \end{aligned} \tag{A.1}$$

which has a unique 0-1 valued solution $(v_0^*, v_1^*, v_2^*, v_3^*) = (1, 0, 0, 0)$. For each equality in a given system $A\boldsymbol{z} = \mathbf{1}_p$, we construct three equalities as follows. We introduce a specified variable z_0. We denote the ℓ-th equality of $A\boldsymbol{z} = \mathbf{1}_p$ by $z_i + z_j + z_k = 1$. We introduce a pair of variables (x_ℓ, y_ℓ) and construct three equalities;

$$\begin{aligned} z_i + z_j + x_\ell &= 1, \\ z_k + y_\ell + z_0 &= 1, \\ x_\ell + y_\ell + v_1 &= 1. \end{aligned} \tag{A.2}$$

Here we note that the above system has a 0-1 valued solution $(z_i^*, z_j^*, z_k^*; x_\ell^*, y_\ell^*; z_0^*, v_1^*) = (0, 0, 0; 1, 0; 1, 0)$. By gathering equalities in Eqs. (A.1) and (A.2), we construct a system of equalities, denoted by Q, with $(q + 2p + 5)$ variables and $(3p + 3)$ equalities. The left-hand side of each equality in system Q is the sum of exactly three variables. Obviously, system Q has a 0-1 valued solution $(z_0^*, \boldsymbol{z}^*, \boldsymbol{x}^*, \boldsymbol{y}^*, \boldsymbol{v}^*)$ defined by $z_0^* = 1$, $\boldsymbol{z}^* = \mathbf{0}_q$, $\boldsymbol{x}^* = \mathbf{1}_p$, $\boldsymbol{y}^* = \mathbf{0}_p$ and $(v_0^*, v_1^*, v_2^*, v_3^*) = (1, 0, 0, 0)$.

Let us consider a case that a given system of equalities $A\boldsymbol{z} = \mathbf{1}_p$ has a 0-1 valued solution $\boldsymbol{z}'$. Then, system Q has a solution $(z_0', \boldsymbol{z}', \boldsymbol{x}', \boldsymbol{y}', \boldsymbol{v}')$ defined by $z_0' = 0$, $(v_0', v_1', v_2', v_3') = (1, 0, 0, 0)$ and $x_\ell' = 1 - (z_i' + z_j')$, $y_\ell' = 1 - z_k'$ (where the ℓ-th equality of a given system $A\boldsymbol{z} = \mathbf{1}_p$ is $z_i + z_j + z_k = 1$). The solution satisfies the third equality in Eq. (A.2), since

$$\begin{aligned} x_\ell' + y_\ell' + v_1' &= 1 - (z_i' + z_j') + 1 - z_k' + v_1' \\ &= 2 - (z_i' + z_j' + z_k') + v_1' = 2 - 1 + 0 = 1. \end{aligned}$$

It is obvious that the solution $(z_0', \boldsymbol{z}', \boldsymbol{x}', \boldsymbol{y}', \boldsymbol{v}')$ is different from $(z_0^*, \boldsymbol{z}^*, \boldsymbol{x}^*, \boldsymbol{y}^*, \boldsymbol{v}^*)$.

Lastly, we consider the inverse implication that system Q has a 0-1 valued solution $(z_0', \boldsymbol{z}', \boldsymbol{x}', \boldsymbol{y}', \boldsymbol{v}')$ which is different from $(z_0^*, \boldsymbol{z}^*, \boldsymbol{x}^*, \boldsymbol{y}^*, \boldsymbol{v}^*)$. Obviously, we have that $(v_0', v_1', v_2', v_3') = (v_0^*, v_1^*, v_2^*, v_3^*) = (1, 0, 0, 0)$. Assume on the contrary that $z_0' = 1$. Then, the definition of system (A.2) implies that $(z_i', z_j', z_k'; x_\ell', y_\ell') = (0, 0, 0; 1, 0)$, since $v_1' = 0$. Thus, we have $(z_0', \boldsymbol{z}', \boldsymbol{x}', \boldsymbol{y}', \boldsymbol{v}') = (z_0^*, \boldsymbol{z}^*, \boldsymbol{x}^*, \boldsymbol{y}^*, \boldsymbol{v}^*)$, which contradicts the assumption. Now we have that $z_0' = 0$. The definition of system (A.2) implies that

$$\begin{aligned} z_i' + z_j' + z_j' &= (1 - x_\ell') + (1 - y_\ell' - z_0') = 2 - (x_\ell' + y_\ell') - z_0' \\ &= 2 - (1 - v_1') - z_0' = 2 - (1 - 0) - 0 = 1. \end{aligned}$$

From the above discussion, $\boldsymbol{z}'$ satisfies $A\boldsymbol{z}' = \mathbf{1}_p$, and thus a given system $A\boldsymbol{z} = \mathbf{1}_p$ has a 0-1 valued solution. □

Tomomi Matsui received his B.E., M.E. and Dr. of Science from Tokyo Institute of Technology. He is now a professor at Chuo University. His areas of interests include combinatorial optimization and game theory.