DEPARTMENT OF MATHEMATICS
RADBOUD UNIVERSITY NIJMEGEN The Netherlands

ON THE ASP-COMPLETENESS OF CRYPTARITHMS

Michiel de Bondt

Report No. 0419 (November 2004)

DEPARTMENT OF MATHEMATICS
RADBOUD UNIVERSITY NIJMEGEN
Toernooiveld
6525 ED Nijmegen
The Netherlands

On the ASP-completeness of Cryptarithms

Michiel de Bondt
Radboud University
Nijmegen, The Netherlands
M.deBondt@math.ru.nl

A cryptarithm is something like

$$\begin{array}{r} \text{SEND} \\ \text{MORE} \\ \hline \text{MONEY} \end{array}$$

For the letters, you must substitute distinct digits such that the words become numbers. In the above example, MONEY must be the sum of SEND and MORE.

We only consider cryptarithms of the above type, e.g. with two summands.

D. Eppstein already showed in [1] that Cryptarithms is NP-complete. He reduced from 3-SAT, but did not show ASP-completeness. We reduce from (1 in 3)-SAT instead. See [2] for the meaning of ASP-completeness.

Let us first assume that the letters do not need to be distinct digits. Then we have a variant of cryptarithms which is ASP-complete for any base ≥ 2. The following symbolic digits on the right ensure that $c_i = i$ for all given c_i, where b is the base:

$$\begin{array}{ccccc} \cdots & c_0 & c_0 & c_1 & c_0 \\ \cdots & c_0 & c_0 & c_{b-1} & c_0 \\ \hline \cdots & c_0 & c_1 & c_0 & c_0 \end{array}$$

We write $0, 1, b-1$ instead of c_0, c_1, c_{b-1} from now. Let $a_1, a_2, \ldots, a_n \in \{0, 1\}$ be the variables of our instance of 3-SAT and $a'_i := 1 - a_i$ the inverse of a_i. The following symbolic digits enforce that $a_i \in \{0, 1\}$ and $a'_i = 1 - a_i$:

$$\begin{array}{ccccc} \cdots & 0 & a_i & 0 & \cdots \\ \cdots & 0 & a'_i & 0 & \cdots \\ \hline \cdots & 0 & 1 & 0 & \cdots \end{array}$$

Say that the jth equation denotes $a'_2 + a_4 + a_7 = 1$ (all others are similar). This equation can be coded as

$$\begin{array}{ccccccc} \cdots & 0 & t_j & 0 & a'_2 & 0 & \cdots \\ \cdots & 0 & a_7 & 0 & a_4 & 0 & \cdots \\ \hline \cdots & 0 & 1 & 0 & t_j & 0 & \cdots \end{array}$$

So we can reduce (1 in 3)-SAT to cryptarithms without distinct digits for any base ≥ 2.

Next, we show that Cryptarithms with distinct digits is ASP-complete, again by reducing from (1 in 3)-SAT. Since there are only $b!$ possibilities to check, the base b can not be bounded. Again, write $a_1, a_2, \ldots, a_n$ for the variables of an arbitrary instance of (1 in 3)-SAT and $a'_1, a'_2, \ldots, a'_n$ for their inverses.

Take the base b at least $8(n^2 + 3n + 1)$ such that $4 \mid b$. We will use the following symbolic digits:

- $c_0 = 0$, $c_4 = 4$, $c_8 = 8$, $\ldots$, $c_{b-4} = b - 4$ and $c_1 = 1$ and $c_2 = 2$,

- $\bar{a}_i = a_i + 4i + 1$, $\bar{a}'_i = a'_i + 4i + 1$, $\hat{a}_i = a_i + 4(n+1)i + 1$ and $\hat{a}'_i = a'_i + 4(n+1)i + 1$, for all i with $1 \leq i \leq n$,

- $d_i = 4(n(n+2) + i) + 2 + a_i b/2$ and $d'_i = 4(n(n+2) + i) + 2 + a'_i b/2$ for all i with $1 \leq i \leq n$,

- $t_{i,j} = \min(\bar{a}_i + \hat{a}_j, \bar{a}'_i + \hat{a}'_j)$ and $t_{i,j} = \min(\bar{a}_i + \hat{a}'_j, \bar{a}'_i + \hat{a}_j)$ for some $i \neq j$ with $1 \leq i, j \leq n$.

If the rightmost part of the cryptaritm looks like

$$
\begin{array}{cccccccccccccccc}
\cdots & c_0 & c_0 & c_{b-4} & c_0 & c_{b-8} & c_0 & \cdots & c_0 & c_8 & c_0 & c_4 & c_0 & c_2 & c_0 & c_1 & c_0 \\
\cdots & c_0 & c_0 & c_4 & c_0 & c_4 & c_0 & \cdots & c_0 & c_4 & c_0 & c_4 & c_0 & c_2 & c_0 & c_1 & c_0 \\
\hline
\cdots & c_0 & c_1 & c_0 & c_0 & c_{b-4} & c_0 & \cdots & c_0 & c_{12} & c_0 & c_8 & c_0 & c_4 & c_0 & c_2 & c_0
\end{array}
$$

then the base b and all c_i are determined. Again, we write i instead of c_i from now. Since the a_i are no digits in our cryptarithm, we may define $a_i := \bar{a}'_i \bmod 2$. The following enforces $\bar{a}_i, \bar{a}'_i, \hat{a}_i, \hat{a}'_i, d_i$ and d'_i to have their given values:

$$
\begin{array}{cccccccccccccccc}
\cdots & 0 & \bar{a}'_i & d_i & 0 & d_i & 0 & \bar{a}_i & d'_i & 0 & 0 & \bar{a}_i & 0 & \bar{a}'_i & 0 & \cdots \\
\cdots & 0 & 2 & d_i & 0 & d'_i & 0 & 2 & d'_i & 0 & 0 & 4ni & 0 & 4ni & 0 & \cdots \\
\hline
\cdots & 0 & 4i+4 & 8(n(n+2)+i)+4 & 0 & 8(n(n+2)+i)+4+b/2 & 0 & 4i+4 & 8(n(n+2)+i)+4 & 0 & 0 & \hat{a}_i & 0 & \hat{a}'_i & 0 & \cdots
\end{array}
$$

Since $\bar{a}'_i \equiv a_i \pmod 2$, $d_i + d_i$ relieves a carry if and only if $a_i = 1$ and d_i has the desired value. Next, d'_i is what it should be, so $\bar{a}_i$ also. At last, $\hat{a}_i$ and $\hat{a}'_i$ are determined.

Assume that $a'_k + a_l + a_m = 1$ is an equation of the given instance of (1 in 3)-SAT (all other equations are similar). We code this equation as follows:

$$\begin{array}{ccccccc} \cdots & 0 & t'_{k,l} & 0 & \bar{a}'_k & 0 & \cdots \\ \cdots & 0 & \bar{a}_m & 0 & \hat{a}_l & 0 & \cdots \\ \hline \cdots & 0 & 4(k+(n+1)(l+m))+4 & 0 & t'_{k,l} & 0 & \cdots \end{array}$$

This enforces the equation $a'_k + a_l + a_m = 1$ to be satisfied. Next, assume that $a_k + a'_l + a_p = 1$ is another such equation. If we code this equation, we use the same variable $t'_{k,l}$ as above, which might seem odd. But, since

$$2 = (a_k + a'_k) + (a_l + a'_l) \leq (a'_k + a_l + a_m) + (a_k + a'_l + a_p) = 2$$

it follows that $a'_k + a_l = a_k + a'_l = 1$ and $a_m = a_p = 0$. Consequently, $\bar{a}'_k + \hat{a}_l = \bar{a}_k + \hat{a}'_l = t'_{k,l}$.

So we only need to show that no collisions of symbolic digits occur, i.e. all symbolic digits are distinct. Notice first that every sum of at most one $\bar{a}_i$ and at most one $\hat{a}_j$ is different, since $(i,j) \mapsto 4i + 4(n+1)j$ is injective if $0 \leq i,j \leq n$. So all $\bar{a}_i, \bar{a}'_i, \hat{a}_j, \hat{a}'_j, t_{i,j}, t'_{i,j}$ are different. Furthermore, the d_i and d'_i are larger than $4(n+1)^2$, so they are larger than all previous symbolic digits. $\min(d_n, d'_n) = 4n(n+3)+2$ must not relieve a carry when added to itself, so $b > 8n(n+3)+4$ i.e. $b \geq 8(n^2+3n+1)$.

References

[1] D. Eppstein, On the NP-completeness of cryptarithms, *SIGACT News* **18** (3) (1987) 38-40.

[2] T. Yato and T. Seta, Complexity and Completeness of Finding Another Solution and its Applications to Puzzles, *IEICE Trans. Fundamentals*, Vol. E86-A, No. 5, pp. 1052-1060, 2003.