# On the ASP-completeness of Cryptarithms 

Michiel de Bondt<br>Radboud University<br>Nijmegen, The Netherlands<br>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. Furthermore, his proof relies on a classical combinatorial result. 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 $\geq 2$. 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 $a_{i}^{\prime}:=1-a_{i}$ the inverse of $a_{i}$. The following symbolic digits enforce that $a_{i} \in\{0,1\}$ and $a_{i}^{\prime}=1-a_{i}$ :

$$
\begin{array}{ccccc}
\cdots & 0 & a_{i} & 0 & \cdots \\
\cdots & 0 & a_{i}^{\prime} & 0 & \cdots \\
\hline \cdots & 0 & 1 & 0 & \cdots
\end{array}
$$

Say that the $j$ th equation denotes $a_{2}^{\prime}+a_{4}+a_{7}=1$ (all others are similar). This equation can be coded as

$$
\begin{array}{ccccccc}
\cdots & 0 & t_{j} & 0 & a_{2}^{\prime} & 0 & \cdots \\
\cdots & 0 & a_{7} & 0 & a_{4} & 0 & \cdots \\
\hline \cdots & 0 & 1 & 0 & t_{j} & 0 & \cdots
\end{array}
$$

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

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 $a_{1}^{\prime}, a_{2}^{\prime}, \ldots, a_{n}^{\prime}$ for their inverses.

Take the base $b$ at least $8\left(n^{2}+3 n+1\right)$ 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 $c_{2}=2$,
- $\bar{a}_{i}=a_{i}+4 i+1, \bar{a}_{i}^{\prime}=a_{i}^{\prime}+4 i+1, \hat{a}_{i}=a_{i}+4(n+1) i+1$ and $\hat{a}_{i}^{\prime}=$ $a_{i}^{\prime}+4(n+1) i+1$, for all $i$ with $1 \leq i \leq n$,
- $d_{i}=4(n(n+2)+i)+2+a_{i} b / 2$ and $d_{i}^{\prime}=4(n(n+2)+i)+2+a_{i}^{\prime} b / 2$ for all $i$ with $1 \leq i \leq n$,
- $t_{i, j}=\min \left(\bar{a}_{i}+\hat{a}_{j}, \bar{a}_{i}^{\prime}+\hat{a}_{j}^{\prime}\right)$ and $t_{i, j}=\min \left(\bar{a}_{i}+\hat{a}_{j}^{\prime}, \bar{a}_{i}^{\prime}+\hat{a}_{j}\right)$ for some $i \neq j$ with $1 \leq i, j \leq n$.

If the rightmost part of the cryptaritm looks like

$$
\begin{array}{lcccccccccccccccc}
\cdots & c_{0} & c_{0} & c_{b-4} & c_{0} & c_{b-8} & c_{0} & \cdots & c_{0} & c_{8} & c_{0} & c_{4} & c_{0} & c_{2} & c_{0} & c_{1} & c_{0} \\
\cdots & c_{0} & c_{0} & c_{4} & c_{0} & c_{4} & c_{0} & \cdots & c_{0} & c_{4} & c_{0} & c_{4} & c_{0} & c_{2} & c_{0} & c_{1} & c_{0} \\
\hline \cdots & c_{0} & c_{1} & c_{0} & c_{0} & c_{b-4} & c_{0} & \cdots & c_{0} & c_{12} & c_{0} & c_{8} & c_{0} & c_{4} & c_{0} & c_{2} & c_{0}
\end{array}
$$

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 $a_{i}:=\bar{a}_{i}^{\prime} \bmod 2$. The following enforces $\bar{a}_{i}, \bar{a}_{i}^{\prime}, \hat{a}_{i}, \hat{a}_{i}^{\prime}, d_{i}$ and $d_{i}^{\prime}$ to have their
given values:


Since $\bar{a}_{i}^{\prime} \equiv a_{i}(\bmod 2), d_{i}+d_{i}$ relieves a carry if and only if $a_{i}=1$ and $d_{i}$ has the desired value. Next, $d_{i}^{\prime}$ is what it should be, so $\bar{a}_{i}$ also. At last, $\hat{a}_{i}$ and $\hat{a}_{i}^{\prime}$ are determined.

Assume that $a_{k}^{\prime}+a_{l}+a_{m}=1$ is an equation of the given instance of ( 1 in 3)-SAT (all other equations are similar). We code this equation as follows:


This enforces the equation $a_{k}^{\prime}+a_{l}+a_{m}=1$ to be satisfied. Next, assume that $a_{k}+a_{l}^{\prime}+a_{p}=1$ is another such equation. If we code this equation, we use the same variable $t_{k, l}^{\prime}$ as above, which might seem odd. But, since

$$
2=\left(a_{k}+a_{k}^{\prime}\right)+\left(a_{l}+a_{l}^{\prime}\right) \leq\left(a_{k}^{\prime}+a_{l}+a_{m}\right)+\left(a_{k}+a_{l}^{\prime}+a_{p}\right)=2
$$

it follows that $a_{k}^{\prime}+a_{l}=a_{k}+a_{l}^{\prime}=1$ and $a_{m}=a_{p}=0$. Consequently, $\bar{a}_{k}^{\prime}+\hat{a}_{l}=\bar{a}_{k}+\hat{a}_{l}^{\prime}=t_{k, l}^{\prime}$.

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 $(i, j) \mapsto 4 i+4(n+1) j$ is injective if $0 \leq i, j \leq n$. So all $\bar{a}_{i}, \bar{a}_{i}^{\prime}, \hat{a}_{j}, \hat{a}_{j}^{\prime}, t_{i, j}, t_{i, j}^{\prime}$ are different. Furthermore, the $d_{i}$ and $d_{i}^{\prime}$ are larger than $4(n+1)^{2}$, so they are larger than all previous symbolic digits. $\min \left(d_{n}, d_{n}^{\prime}\right)=4 n(n+3)+2$ must not relieve a carry when added to itself, so $b>8 n(n+3)+4$ i.e. $b \geq 8\left(n^{2}+3 n+1\right)$.

## 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.

