4.4 Example: Presburger arithmetic

We have seen that particularly weak monadic second-order logic on finite words ($WS1S$) is decidable. We use this result to prove the decidability of *Presburger arithmetic*, i.e. the set of first-order formulas that are true on $(\mathbb{N}, +)$.

The first approach is through the logic. Since a number can be represented as a binary sequence $\sum_{i=0}^{k} a_i 2^i$, we can define a corresponding set of those i for which $a_i = 1$. For example, let us take the number 6, the reverse of its binary representation is then 011 and the corresponding subset is then $\{1, 2\}$. For the length of the word we take the greatest i such that there is a number having i in its subset representation.

We now need to express the addition using $WMF_2(S)$. Precisely to find a formula $\mathrm{Plus}(X, Y, Z) \in WMF_2(S)$ that is true iff $x + y = z$, where x, y, z are numbers corresponding to X, Y, Z, respectively. For this, we simulate the algorithm for summing digit by digit with an additional auxiliary subset T to keep the carry bits. Firstly, we express the formula that the sum on a particular place is correct. This is true iff the odd number of summands carries 1.

$$\mathrm{Sum}(a) \equiv ((a \in X \wedge a \notin Y \wedge a \notin T) \vee (a \notin X \wedge a \in Y \wedge a \notin T)$$

$$\vee (a \notin X \wedge a \notin Y \wedge a \in T) \vee (a \in X \wedge a \in Y \wedge a \in T)) \leftrightarrow a \in Z$$

where $\varphi \leftrightarrow \psi \equiv (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$. The formula that the carry bit is 1 is true iff at least two summands carry 1. Note that if overall overflow should happen, the formula is correctly false by the existential quantification.

$$\mathrm{Carry}(a) \equiv ((a \in X \wedge a \in Y) \vee (a \in X \wedge a \in T)$$

$$\vee (\wedge a \in Y \wedge a \in T)) \leftrightarrow \exists b(S(a, b) \wedge b \in T)$$

Now, we are able to express the summing of two numbers. It is necessary to ensure that the first carry bit is 0.

$$\mathrm{Plus}(X, Y, Z) = \exists T \forall a(\mathrm{Sum}(a) \wedge \mathrm{Carry}(a) \wedge ((\neg \exists b(S(a, b))) \rightarrow a \notin T))$$

Thus, we can translate any first-order formula with signature $+$ to an equivalent $WMF_2(S)$ formula: the first-order quantification is replaced by the subset quantification and $+$ by Plus. The same holds for sentences, thus proving Presburger arithmetic decidable by the decidability of $WMF_2(S)$.

The second approach to prove this is to find the respective automaton using a similar idea as in the proof of Büchi theorem. We use an alphabet

$\{0,1\}^n$, where n is the number of variables. We use the same representation as above and the same summing algorithm.

We can imagine one head per each component and all moving synchronously when reading. What we can check is then called synchronized rational relation. Since we are over the base 2, we call them *2-recognizable relations*. A question arises: What should we add to Presburger arithmetic to make it as strong as automata and WMF_2? The answer is: A predicate associating with each number $m > 0$ the greatest power of 2 which divides m.