Embedding quadratization gadgets for reduction by substitution

Nike Dattani[*]
Harvard-Smithsonian Center for Astrophysics

Consider the symmetric function:

$$b_1b_2b_3 + b_2b_3b_4 + b_3b_4b_1 + b_4b_1b_2 \tag{1}$$

We will *re-use* auxiliary variables by pairing variables appropriately:

$$\color{red}{b_1b_2}\color{black}{b_3 + b_2}\color{green}{b_3b_4}\color{black}{ + }\color{green}{b_3b_4}\color{black}{b_1 + b_4}\color{red}{b_1b_2} \tag{2}$$

Here only 2 auxiliary variables are required in total. This is *more* than BCR which requires only 1 auxiliary ($\lceil \log k \rceil - 1$ auxiliary qubits for a degree k function in general). However, BCR is fully connected (K_5) and Chau's graph (Ch_6) for the RBS is not. K_5 requires one auxiliary qubit on pegasus (see paper: https://arxiv.org/pdf/1901.07676.pdf). **How many does Ch_6 require? K_5can be embedded in Pegasus with a total of 6 qubits in a single cell. Can Ch_6 do that?**

Let us continue with all possible cubic terms, but with 5 variables instead of 4:

$$b_1b_2b_3 + b_2b_3b_4 + b_3b_4b_5 + b_4b_5b_1 + b_5b_1b_2 \tag{3}$$

Now 3 auxuliary variables are required in total:

$$\color{red}{b_1b_2}\color{black}{b_3 + b_2c + }\color{green}{b_3b_4}\color{black}{b_5 + }\color{blue}{b_4b_5}\color{black}{b_1 + b_5}\color{red}{b_1b_2} \tag{4}$$

this means the graph will be Ch_8 as opposed to K_7 (2 auxiliary, 5 logical) in the case of BCR. **My guess is that Ch_8 (8 variables) is much easier to embed than K_7 (7 variables).**

Let us now try with $n = 6$ and $k = 3$:

$$b_1b_2b_3 + b_2b_3b_4 + b_3b_4b_5 + b_4b_5b_6 + b_5b_6b_1 + b_6b_1b_2 \tag{5}$$

$$= \color{red}{b_1b_2}\color{black}{b_3 + b_2}\color{green}{b_3b_4}\color{black}{ + }\color{green}{b_3b_4}\color{black}{b_5 + b_4}\color{blue}{b_5b_6}\color{black}{ + }\color{blue}{b_5b_6}\color{black}{b_1 + b_6}\color{red}{b_1b_2} \tag{6}$$

We therefore only need auxiliaries, plus the 6 original logicals, meaning that we have Ch_9, compared to K_8 for BCR. Ch_9 **definitely wins here!**

This analysis is staight-forward to contunue to larger n and $k = 3$.
Let's now look at $n = 5$ and $k = 4$:

$$b_1b_2b_3b_4 + b_2b_3b_4b_5 + b_3b_4b_5b_1 + b_4b_5b_1b_2 + b_5b_1b_2b_3. \tag{7}$$

Here we will pair some variables again (2 auxiliaries):

$$\color{red}{b_1b_2}\color{green}{b_3b_4}\color{black}{ + b_2}\color{green}{b_3b_4}\color{black}{b_5 + }\color{green}{b_3b_4}\color{black}{b_5b_1 + b_4b_5}\color{red}{b_1b_2}\color{black}{ + b_5}\color{red}{b_1b_2}\color{black}{b_3} \tag{8}$$

$$= \color{red}{b_{a_{12}}}\color{green}{b_{a_{34}}}\color{black}{ + b_2}\color{green}{b_{a_{34}}}\color{black}{b_5 + }\color{green}{b_{a_{34}}}\color{black}{b_5b_1 + b_4b_5}\color{red}{b_{a_{12}}}\color{black}{ + b_5}\color{red}{b_{a_{12}}}\color{black}{b_3} \tag{9}$$

[*] n.dattani@cfa.harvard.edu

We cannot pair anymore variables, so we need 4 more auxiliaries. In total we have 6 auxiliaries plus 5 logical variables, meaning we have Ch_{11}. For BCR we have only 1 auxiliary variable, so it is K_6 vs Ch_{11}. K_6 **probably wins because it only need 2 auxiliary qubits for pegasus on a single cell. It is impossible for Ch_{11} to work on a single cell.**

Now let's look at $n = 6$ and $k = 5$:

$$b_1b_2b_3b_4b_5 + b_2b_3b_4b_5b_6 + b_3b_4b_5b_6b_1 + b_4b_5b_6b_1b_2 + b_5b_6b_1b_2b_3 + b_6b_1b_2b_3b_4. \tag{10}$$

Let us introduce 3 auxuliuaries:

$$b_1b_2b_3b_4b_5 + b_2b_3b_4b_5b_6 + b_3b_4b_5b_6b_1 + b_4b_5b_6b_1b_2 + b_5b_6b_1b_2b_3 + b_6b_1b_2b_3b_4 \tag{11}$$
$$= b_{a_{12}}b_{a_{34}}b_5 + b_2b_{a_{34}}b_{a_{56}} + b_{a_{34}}b_{a_{56}}b_1 + b_4b_{a_{56}}b_{a_{12}} + b_{a_{56}}b_{a_{12}}b_3 + b_6b_{a_{12}}b_{a_{34}} \tag{12}$$

Let us now pair up some of the auxiliary qubits!

$$b_{a_{12}a_{34}}b_5 + b_2b_{a_{34}a_{56}} + b_{a_{34}a_{56}}b_1 + b_4b_{a_{56}a_{12}} + b_{a_{56}a_{12}}b_3 + b_6b_{a_{12}a_{34}}$$

This is now quadratic, with 6 total auxiliaries and 6 original logicals. We therefore have Ch_{12}, compared to K_8 with BCR. **It is my guess that Ch_{12} will win for Pegasus. K_8 will not be easy at all.**