Problem 7. «s-Boolean sharing»

In cryptography, a field known as **side-channel analysis** uses extra information such as the power consumption of an implementation to break a cryptographic primitive. In order to defend against these attacks, one does not need to change the primitive but only the way the primitive is implemented. A popular countermeasure is called "**sharing**" where the computation of the primitive is split in multiple parts. Each part seemingly operates on random data such that an adversary has to observe all parts of the computation in order to gain sense of the secret information that was processed.

- An s-**Boolean sharing of a variable** $x \in \mathbb{F}_2$ is a vector $(x_1, x_2, ..., x_s) \in \mathbb{F}_2^s$ such that $x = \bigoplus_{i=1}^s x_i$.
- A vectorial Boolean function $G : \mathbb{F}_2^{sn} \to \mathbb{F}_2^{sm}$ is an s-**Boolean sharing of a function** $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ if for all $x \in \mathbb{F}_2^n$ and $(x_1, ..., x_s) \in \mathbb{F}_2^{sn}$, $x_i \in \mathbb{F}_2^n$, such that $\bigoplus_{i=1}^s x_i = x$,

$$\bigoplus_{i=1}^{s} G_i(x_1, ..., x_s) = F(x)\,.$$

Here, $G = (G_1, ..., G_s)$, where $G_i : \mathbb{F}_2^{sn} \to \mathbb{F}_2^m$ and "$\oplus$" denotes the bit-wise XOR.

Q1 Write an algorithm which takes in a vectorial Boolean function and an integer s and returns true/false on whether the function is a s-Boolean sharing of another function. In case the result is true, the algorithm also returns the function whose sharing is the algorithm's input.

Q2 Problem for a special prize! Propose a theoretical solution to the problem of checking whether the function is a s-Boolean sharing of another function.

Example. If you give the Boolean function $G : \mathbb{F}_2^6 \to \mathbb{F}_2^3$ such that

$$\begin{aligned}G_1(a,b,c,d,e,f) &= ad \oplus ae \oplus bd\\ G_2(a,b,c,d,e,f) &= be \oplus bf \oplus ce\\ G_3(a,b,c,d,e,f) &= cf \oplus cd \oplus af\end{aligned}$$

the algorithm should return true when $s = 3$ together with the function $F : \mathbb{F}_2^2 \to \mathbb{F}_2$ such that $F(x, y) = xy$, where $x = a \oplus b \oplus c$ and $y = d \oplus e \oplus f$.