Retrodictive Execution of Quantum Circuits

Jacques Carette McMaster University
Gerardo Ortiz* Indiana University
Amr Sabry Indiana University

February 2, 2022

Abstract

1 Introduction

> You can't connect the dots looking forward; you can only connect them looking backwards. So you have to trust that the dots will somehow connect in your future. Steve Jobs

Retrodictive quantum theory [2], retrocausality [1], and the time-symmetry of physical laws [5] suggest that partial knowledge about the future can be exploited to understand the present. We demonstrate the even stronger proposition that, in concert with the computational concepts of *demand-driven lazy evaluation* [4] and *symbolic partial evaluation* [3], retrodictive reasoning can be used to de-quantize some quantum algorithms, i.e., to provide efficient classical algorithms inspired by their quantum counterparts.

We begin by introducing the principles of demand-driven lazy evaluation, symbolic partial evaluation, and then apply them to the quantum circuit model to de-quantize quantum algorithms.

Lazy Evaluation. Consider a program that searches for three different numbers x, y, and z each in the range $[1..n]$ and that sum to s. A well-established design principle for solving such problems is the *generate-and-test* computational paradigm. Following this principle, a simple program to solve this problem in the programming language Haskell is:

```
generate :: Int -> [(Int,Int,Int)]
generate n =  [(x,y,z) | x <- [1..n], y <- [1..n], z <- [1..n]]

test :: Int -> [(Int,Int,Int)] -> [(Int,Int,Int)]
test s nums = [(x,y,z) | (x,y,z) <- nums, x /= y, x /= z, y /= z, x+y+z == s]

find :: Int -> Int -> (Int,Int,Int)
find s =  head . test s . generate
```

The program consists of three functions: `generate` that produces all triples `(x,y,z)` from `(1,1,1)` to `(n,n,n)`; `test` that checks that the numbers are different and that their sum is equal to `s`; and `find` that composes the two functions: generating all triples, testing the ones that satisfy the condition, and returning the first solution. Running this program to find numbers in the range [1..6] that sum to 15 immediately produces $(4, 5, 6)$ as expected. But what if the range of interest was [1..10000000] ? A naïve execution of the generate-and-test method would be prohibitively expensive as it would spend all its time generating an enormous number of triples that are un-needed.

Lazy demand-driven evaluation as implemented in Haskell succeeds in a few seconds with the result $(1, 2, 12)$, however. The idea is simple: instead of eagerly generating all the triples, generate a process that,

when queried, produces one triple at a time on demand. Conceptually the execution starts from the observer side which is asking for the first element of a list; this demand is propagated to the function `test` which itself propagates the demand to the function `generate`. As each triple is generated, it is tested until one triple passes the test. This triple is immediately returned without having to generate any additional values.

Partial Evaluation. Below is a Haskell program that computes a^n by repeated squaring:

```
power :: Int -> Int -> Int
power a n
  | n == 0     = 1
  | n == 1     = a
  | even n     = let r = power a (n `div` 2) in r * r
  | otherwise  = a * power a (n-1)
```

When both inputs are known, e.g., `a = 3` and `n = 5`, the program evaluates as follows:

```
   power 3 5
=  3 * power 3 4
=  3 * (let r1 = power 3 2 in r1 * r1)
=  3 * (let r1 = (let r2 = power 3 1 in r2 * r2) in r1 * r1)
=  3 * (let r1 = (let r2 = 3 in r2 * r2) in r1 * r1)
=  3 * (let r1 = 9 in r1 * r1)
=  243
```

Partial evaluation is used when we only have partial information about the inputs. Say we only know $n = 5$. A partial evaluator then attempts to evaluate `power` with symbolic input `a` and actual input `n=5`. This evaluation proceeds as follows:

```
   power a 5
=  a * power a 4
=  a * (let r1 = power a 2 in r1 * r1)
=  a * (let r1 = (let r2 = power a 1 in r2 * r2) in r1 * r1)
=  a * (let r1 = (let r2 = a in r2 * r2) in r1 * r1)
=  a * (let r1 = a * a in r1 * r1)
=  let r1 = a * a in a * r1 * r1
```

All of this evaluation, simplification, and specialization happens without knowledge of `a`. Just knowing `n` was enough to produce a residual program that is much simpler.

Quantum Circuit Model. Many quantum algorithms can be expressed using circuits consisting of three stages: preparation, unitary evolution, and measurement. For a large number of quantum algorithms, the unitary evolution is a quantum oracle U_f that encapsulates a classical function f to be analyzed as shown in Fig. 1.

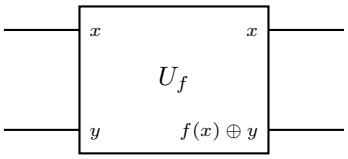


Figure 1: Quantum oracle

In the conventional execution model of quantum circuits, which is the conventional way to use quantum mechanics as a predictive theory, the U_f block receives both inputs and evolves in the forwards direction to produce the outputs. The preceding discussion about lazy evaluation and partial evaluation suggests, however, more creative ways to execute the U_f block as shown in Fig. 2. In this scenario, the second register has both a known initial and final observed result. Using this knowledge, it is possible to perform a demand-driven partial evaluation with a symbolic placeholder for x. This execution produces information about the necessary initial conditions on x that lead to the observed final result..

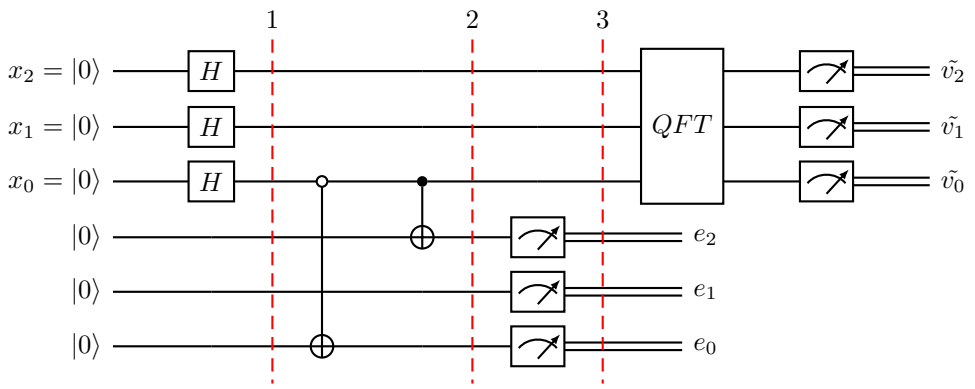


Figure 3: Finding the period of $4^x \mod 15$

The circuit in Fig. 3 explains the idea in a simple but realistic scenario. The circuit uses a hand-optimized U_f that implements the modular exponentiation $4^x \mod 15$ in order to factor 15 using Shor's algorithm. In a conventional setting, the execution proceeds as follows. At step (1), we have the initial state $(1/2\sqrt{2})\sum_{i=0}^{7}|i\rangle|0\rangle$. The state evolves through the U_f block between (1) and (2) to become:

$$\frac{1}{2\sqrt{2}}((|0\rangle+|2\rangle+|4\rangle+|6\rangle)|1\rangle+(|1\rangle+|3\rangle+|5\rangle+|7\rangle)|4\rangle)$$

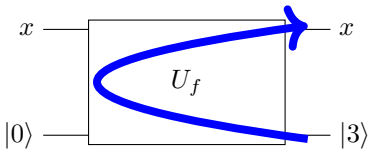


Figure 2: Retrodictive execution flow

At this point, the second register is measured. The result of the measurement can be either $|1\rangle$ or $|4\rangle$. In either case, the top register snaps to a state of the form $\sum_{r=0}^{3}|a+2r\rangle$ whose QFT has peaks at $|0\rangle$ or $|4\rangle$. If we measure $|0\rangle$ we repeat the experiment; otherwise we infer that the period is 2.

Instead of this forward execution, we can reason as follows. Since $x^0 = 1$ for all x, we know that $|1\rangle$ is a possible measurement of the second register. We can therefore proceed in a retrodictive fashion with the state $|x_2x_1x_0\rangle|001\rangle$ at step 2 and computing backwards. In this symbolic execution, the first CX-gate changes the state to $|x_2x_1x_0\rangle|x_001\rangle$ and the second CX-gate produces $|x_2x_1x_0\rangle|x_0x_0\rangle$. At that point, we reconcile the retrodictive result of the second register $|x_0x_0\rangle$ with the initial condition $|000\rangle$ to conclude that $x_0 = 0$. In other the first register must be in a superposition of basis states of the form $|??0\rangle$ where the least significant bit must be 0 and the other two bits are unconstrained. Expanding the possibilities, the first register need to be in a superposition of the states $|000\rangle, |010\rangle, |100\rangle$ or $|110\rangle$. We have just inferred, using purely classical but retrodictive reasoning, that the period is 2.

In order to assess whether this idea works for a broader class of situations including different algorithms and different circuit sizes, we implemented the demand-driven symbolic partial evaluator and ran it on a variety of circuits. The first experiment generalizes the simple example above by using more qubits and circuits that are constructed automatically without any manual optimization. In particular, we generated 8 qubit modular exponentiations circuits to compute $a^x \mod 15$ for $a \in \{2,4,7,8,11,13,14\}$. Each of the circuits, automatically constructed from first principles using adders and multipliers, has 26244 CX(controlled not) gates, 27378 CCX(Toffoli) gates, and 2916 CCCX (generalized Toffoli) gates. Running the retrodictive partial evaluator with an observed value of 1, produces the equations in Fig. 4.

Perhaps surprisingly, even though there are 8 qubits in the circuit and thousands of controlled gates, the equations are trivial and immediately solvable as they only involve either the least significant bit x_0 (when $a \in \{4,11,14\}$) or the least significant two bits x_0 and x_1 (when $a \in \{2,7,8,13\}$). When the solution is $x_0 = 0$, the period is 2. When the solution is $x_0 = 0, x_1 = 0$, the period is 4.

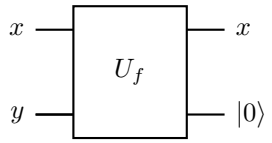
It turns that retrodictive symbolic evaluation is powerful enough to solve some instances of Deutsch-Jozsa, Bernstein-Vazirnani, and Simon problems, as well as some instances of Grover's and Shor's algorithms.

$a = 11$	$x_0 = 0$				$\mid x_0 = 0$
$a = 4, 14$	$1 \oplus x_0 = 1$	$x_0 = 0$			$\mid x_0 = 0$
$a = 7, 13$	$1 \oplus x_0 x_1 \oplus x_1 = 1$	$x_0 x_1 = 0$	$x_0 \oplus x_0 x_1 \oplus x_1 = 0$	$x_0 \oplus x_0 x_1 = 0$	$\mid x_0 = 0, x_1 = 0$
$a = 2, 8$	$1 \oplus x_0 \oplus x_0 x_1 \oplus x_1 = 1$	$x_0 x_1 = 0$	$x_0 x_1 \oplus x_1 = 0$	$x_0 \oplus x_0 x_1 = 0$	$\mid x_0 = 0, x_1 = 0$

Figure 4: Equations generated by retrodictive execution of $a^x \mod 15$ starting from observed result 1 and unknown $x_7 x_6 x_5 x_4 x_3 x_2 x_1 x_0$. The solution for the unknown variables is given in the last column.

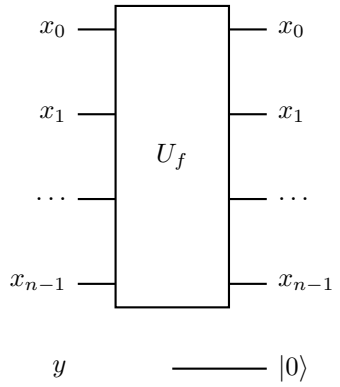
1.1 Deutsch-Jozsa

The problem is to determine if a function $[\mathbf{2}] \to [\mathbf{2}]$ is constant or balanced. The only relevant part of the circuit is:



We fix the ancillary output to a possible boundary condition, say $|0\rangle$, and perform a retrodictive execution of the circuit. This execution produces a formula for y that depends on the function f in the black box. When the function f is a constant function, the formula is the corresponding constant 0 or 1. When the function is balanced the resulting formula is x (when the function is the identity) or $1 + x$ (when the function is boolean negation).

The problem is a generalization of the previous one: the question is to determine if a function $\mathbb{B}^n \to \mathbb{B}$ is constant or balanced. The circuit is identical to above except that x is now a collection of qubits:



Again, we fix the ancillary output to a possible boundary condition, say $|0\rangle$, and perform a retrodictive execution of the circuit. This execution produces a formula for y that depends on the function f in the black box. When the function f is a constant function, the formula is the corresponding constant 0 or 1. When the function is balanced the resulting formula involves at least one variable x_i.

Running retro in deutsch gives:

```
> retroDeutsch deutschId
x

> retroDeutsch deutschNot
```

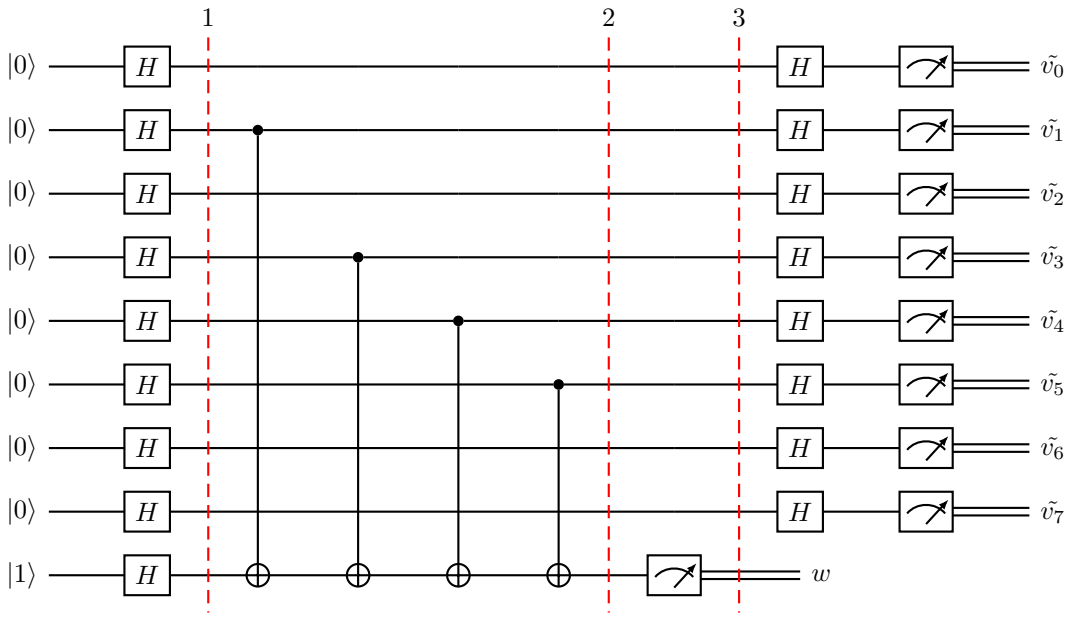


Figure 5: Example Circuit for Bernstein-Vazirani Algorithm

```
1 + x

> retroDeutsch deutsch0
0

> retroDeutsch deutsch1
1
```

Show experiments for Deutsch Jozsa

Bernstein-Vazirani. We are given a function $f : [\mathbf{2^n}] \to [\mathbf{2}]$ that hides a secret number $s \in [\mathbf{2^n}]$. We are promised the function is defined using the binary representations $\sum_i^{n-1} x_i$ and $\sum_i^{n-1} s_i$ of x and s respectively as follows:

$$f(x) = \sum_{i=0}^{n-1} s_i x_i \mod 2$$

The goal is to determine the secret number s.

Expressing the problem as a pre-image calculation is slightly more involved than in the previous two cases. To determine s, we make n queries to the pre-image of a value in the range of the function. Query i asks whether 2^i is a member of the pre-image and the answer determines bit i of the secret s. Indeed, by definition, $f(2^i) = s_i$ and hence s_i is 1 iff 2^i is a member of the pre-image of 1.

The circuit in Fig. 6 solves the problem for $n = 8$ and a hidden number 92 (= 00111010 in binary notation). As required, the circuit between slice (1) and slice (2), collects the sum of the x_i at positions that match the occurrences of 1 in the secret string. The evolution proceeds as follows. At slice (1), the top 8 qubits are each in the state $|+\rangle$ and the bottom qubit is in the state $|-\rangle$, i.e., the state is $(1/3)\ |+++++++-\rangle$. In the evolution between slices (1) and (2), qubits 0, 2, 6, and 7 are untouched and remain in the state $|+\rangle$. Each of the other four qubits becomes $|-\rangle$ as the phase of the target qubit is kicked back to the control qubit by the CX operation. The full state at slice (2) is $(1/3)\ |+-+---++-\rangle$. At this point, we perform

a measurement on the bottom qubit which returns 0 or 1 with equal probability. This measurement causes collapses the top 8 qubits to $\pm(1/2\sqrt{2})\ |+-+---++\rangle$. After applying all the Hadamard gates, the measurement is deterministically $|01011100\rangle$ with the most significant bit at the right. This is the secret number.

Instead of this execution model, we now explore an alternative execution that starts from the observation w and proceeds from slice (2) back towards slice (1) collecting the information necessary to answer the required pre-image query. As explained in the previous section, the secret number can be reconstructed once we know, for each i, whether the number 2^i is a member of the pre-image. When expressed in terms of bits, this means that we need to know, for each bit position i, whether the corresponding qubit contributes to the definition of the pre-image. We therefore start a backwards execution starting with the state $|x_0x_1x_2x_3x_4x_5x_6x_7F()\rangle$ where $F()$ expresses that the last qubit has not been shown to depend on any qubit so far and the x_i symbols are placeholders for unknown values. We trace the execution symbolically:

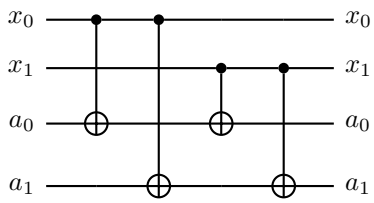
$$\begin{aligned} |x_0x_1x_2x_3x_4x_5x_6x_7F()\rangle &\leftarrow |x_0x_1x_2x_3x_4x_5x_6x_7F(x_5)\rangle \\ &\leftarrow |x_0x_1x_2x_3x_4x_5x_6x_7F(x_4,x_5)\rangle \\ &\leftarrow |x_0x_1x_2x_3x_4x_5x_6x_7F(x_3,x_4,x_5)\rangle \\ &\leftarrow |x_0x_1x_2x_3x_4x_5x_6x_7F(x_1,x_3,x_4,x_5)\rangle \end{aligned}$$

For each operation $\textsc{cx}(x,v)$, we add x to the list of variables on which v depends. At the end of the execution, we conclude that x_1, x_3, x_4, and x_5 are the relevant qubits, from which we infer that the secret string must be 00111010.

Simon. We are given a 2-1 function $f : [\mathbf{2^n}] \to [\mathbf{2^n}]$ with the property that there exists an a such $f(x) = f(x \oplus a)$ for all x; the goal is to determine a. When expressed as a computation of pre-images, the problem statement becomes the following. Pick an arbitrary x and compute the pre-image of $f(x)$. It must contain exactly two values one of which is x. The problem then reduces to finding the other value in the pre-image.

We are given a 2-1 function $f : \mathbb{B}^n \to \mathbb{B}^n$ where there exists an a such $f(x) = f(x \oplus a)$ for all x; the goal is to determine a.

The circuit below demonstrates the situation when $n = 2$ and $a = 3$.



The circuit implements the black box $U_f(x,a) = (x, f(x) \oplus a)$. We first pick a random x, say $x = 3$, fix the initial condition $a = 0$ and run the circuit forward. This execution produces, in the second register, the value of $f(x) = 0$. We now run a symbolic retrodictive execution with $a = 0$ at the output site. That execution produces information on all values of a that are consistent with the observed result. In this case, we get: $a_0 = x_0 + x_1$ and $a_1 = x_0 + x_1$. In other words, when $x_0 = x_1$, we have $a = 0$, and when $x_0 \neq x_1$, we have $a = 3$ which is indeed the desired hidden value.

Deutsch-Jozsa. The conventional statement of the problem is to determine if a function $[\mathbf{2}] \to [\mathbf{2}]$ is constant or balanced. An equivalent statement is to answer a query about the cardinality of a pre-image. In this case, if the cardinality of the pre-image of any value in the range is even i.e. 0 or 2, the function must be constant and if it is odd, i.e., it contains just one element, the function must be balanced.

The problem is a generalization of the previous one: the question is to determine if a function $[\mathbf{2^n}] \to [\mathbf{2}]$ for some n is constant or balanced. When expressed as a pre-image computation, the problem reduces to a query distinguishing the following three situations about the pre-image of a value in the range of the

function: is the cardinality of the pre-image equal to 0, 2^n, or 2^{n-1}? In the first two cases, the function is constant and in the last case, the pre-image contains half the values in the domain indicating that the function is balanced.

A couple of success stories then 21 huge then pre-image story; np-complete; not even quantum computer can solve it luckily we don't actually need to solve it; we need stats about it; explain common algos

insight 1: qft does not care about 0+2+4.... vs 1+3+5....

0 0 ? 0 1 ? 1 0 ? 1 1 ?

equiv no matter what ? is ? is used in the computation (don't care about value) others not used so we just need to keep track of which vars are used

run again; refined pe; var used; if used twice then disappears

go back to that stupid paper about logic programming and xor

The equations turn out to be trivial when the period is a power of 2. This occurs when the number to factor is a product of Fermat primes: 3, 5, 17, 257, 65537, ... The equations generated for some of these cases are in Fig. **??**.

Equations generated by retrodictive execution of $4^x \mod 21$ **starting from observed result 1 and unknown** x**.** The circuit consists of 9 qubits, 36400 CX-gates, 38200 CCX-gates, and 4000 CCCX-gates. There are only three equations but each equation is exponentially large.

$$1\oplus x_0\oplus x_0x_1x_2\oplus x_0x_1x_2x_3x_4\oplus x_0x_1x_2x_3x_4x_5x_6\oplus x_0x_1x_2x_3x_4x_5x_6x_7x_8\oplus x_0x_1x_2x_3x_4x_5x_6x_7x_9\oplus x_0x_1x_2x_3x_4x_5x_6x_8\oplus$$
$$x_0x_1x_2x_3x_4x_5x_6x_8x_9 \oplus x_0x_1x_2x_3x_4x_5x_7 \oplus x_0x_1x_2x_3x_4x_5x_7x_8x_9 \oplus x_0x_1x_2x_3x_4x_5x_7x_9 \oplus x_0x_1x_2x_3x_4x_5x_8 \oplus$$
$$x_0x_1x_2x_3x_4x_5x_9\oplus x_0x_1x_2x_3x_4x_6\oplus x_0x_1x_2x_3x_4x_6x_7\oplus x_0x_1x_2x_3x_4x_6x_7x_8\oplus x_0x_1x_2x_3x_4x_6x_7x_8x_9\oplus x_0x_1x_2x_3x_4x_6x_8x_9\oplus$$
$$x_0x_1x_2x_3x_4x_6x_9 \oplus x_0x_1x_2x_3x_4x_7x_8 \oplus x_0x_1x_2x_3x_4x_7x_9 \oplus x_0x_1x_2x_3x_4x_8 \oplus x_0x_1x_2x_3x_4x_8x_9 \oplus x_0x_1x_2x_3x_5 \oplus$$
$$x_0x_1x_2x_3x_5x_6x_7\oplus x_0x_1x_2x_3x_5x_6x_7x_8x_9\oplus x_0x_1x_2x_3x_5x_6x_7x_9\oplus x_0x_1x_2x_3x_5x_6x_8\oplus x_0x_1x_2x_3x_5x_6x_9\oplus x_0x_1x_2x_3x_5x_7\oplus$$
$$x_0x_1x_2x_3x_5x_7x_8 \oplus x_0x_1x_2x_3x_5x_7x_8x_9 \oplus x_0x_1x_2x_3x_5x_8x_9 \oplus x_0x_1x_2x_3x_5x_9 \oplus x_0x_1x_2x_3x_6 \oplus x_0x_1x_2x_3x_6x_7x_8 \oplus$$
$$x_0x_1x_2x_3x_6x_7x_9 \oplus x_0x_1x_2x_3x_6x_8 \oplus x_0x_1x_2x_3x_6x_8x_9 \oplus x_0x_1x_2x_3x_7 \oplus x_0x_1x_2x_3x_7x_8x_9 \oplus x_0x_1x_2x_3x_7x_9 \oplus$$
$$x_0x_1x_2x_3x_8\oplus x_0x_1x_2x_3x_9\oplus x_0x_1x_2x_4\oplus x_0x_1x_2x_4x_5\oplus x_0x_1x_2x_4x_5x_6\oplus x_0x_1x_2x_4x_5x_6x_7\oplus x_0x_1x_2x_4x_5x_6x_7x_8\oplus$$
$$x_0x_1x_2x_4x_5x_6x_7x_8x_9\oplus x_0x_1x_2x_4x_5x_6x_8x_9\oplus x_0x_1x_2x_4x_5x_6x_9\oplus x_0x_1x_2x_4x_5x_7x_8\oplus x_0x_1x_2x_4x_5x_7x_9\oplus x_0x_1x_2x_4x_5x_8\oplus$$
$$x_0x_1x_2x_4x_5x_8x_9 \oplus x_0x_1x_2x_4x_6x_7 \oplus x_0x_1x_2x_4x_6x_7x_8x_9 \oplus x_0x_1x_2x_4x_6x_7x_9 \oplus x_0x_1x_2x_4x_6x_8 \oplus x_0x_1x_2x_4x_6x_9 \oplus$$
$$x_0x_1x_2x_4x_7\oplus x_0x_1x_2x_4x_7x_8\oplus x_0x_1x_2x_4x_7x_8x_9\oplus x_0x_1x_2x_4x_8x_9\oplus x_0x_1x_2x_4x_9\oplus x_0x_1x_2x_5x_6\oplus x_0x_1x_2x_5x_6x_7x_8\oplus$$
$$x_0x_1x_2x_5x_6x_7x_9 \oplus x_0x_1x_2x_5x_6x_8 \oplus x_0x_1x_2x_5x_6x_8x_9 \oplus x_0x_1x_2x_5x_7 \oplus x_0x_1x_2x_5x_7x_8x_9 \oplus x_0x_1x_2x_5x_7x_9 \oplus$$
$$x_0x_1x_2x_5x_8 \oplus x_0x_1x_2x_5x_9 \oplus x_0x_1x_2x_6 \oplus x_0x_1x_2x_6x_7 \oplus x_0x_1x_2x_6x_7x_8 \oplus x_0x_1x_2x_6x_7x_8x_9 \oplus x_0x_1x_2x_6x_8x_9 \oplus$$
$$x_0x_1x_2x_6x_9\oplus x_0x_1x_2x_7x_8\oplus x_0x_1x_2x_7x_9\oplus x_0x_1x_2x_8\oplus x_0x_1x_2x_8x_9\oplus x_0x_1x_3\oplus x_0x_1x_3x_4x_5\oplus x_0x_1x_3x_4x_5x_6x_7\oplus$$
$$x_0x_1x_3x_4x_5x_6x_7x_8x_9\oplus x_0x_1x_3x_4x_5x_6x_7x_9\oplus x_0x_1x_3x_4x_5x_6x_8\oplus x_0x_1x_3x_4x_5x_6x_9\oplus x_0x_1x_3x_4x_5x_7\oplus x_0x_1x_3x_4x_5x_7x_8\oplus$$
$$x_0x_1x_3x_4x_5x_7x_8x_9 \oplus x_0x_1x_3x_4x_5x_8x_9 \oplus x_0x_1x_3x_4x_5x_9 \oplus x_0x_1x_3x_4x_6 \oplus x_0x_1x_3x_4x_6x_7x_8 \oplus x_0x_1x_3x_4x_6x_7x_9 \oplus$$
$$x_0x_1x_3x_4x_6x_8\oplus x_0x_1x_3x_4x_6x_8x_9\oplus x_0x_1x_3x_4x_7\oplus x_0x_1x_3x_4x_7x_8x_9\oplus x_0x_1x_3x_4x_7x_9\oplus x_0x_1x_3x_4x_8\oplus x_0x_1x_3x_4x_9\oplus$$
$$x_0x_1x_3x_5\oplus x_0x_1x_3x_5x_6\oplus x_0x_1x_3x_5x_6x_7\oplus x_0x_1x_3x_5x_6x_7x_8\oplus x_0x_1x_3x_5x_6x_7x_8x_9\oplus x_0x_1x_3x_5x_6x_8x_9\oplus x_0x_1x_3x_5x_6x_9\oplus$$
$$x_0x_1x_3x_5x_7x_8\oplus x_0x_1x_3x_5x_7x_9\oplus x_0x_1x_3x_5x_8\oplus x_0x_1x_3x_5x_8x_9\oplus x_0x_1x_3x_6x_7\oplus x_0x_1x_3x_6x_7x_8x_9\oplus x_0x_1x_3x_6x_7x_9\oplus$$
$$x_0x_1x_3x_6x_8 \oplus x_0x_1x_3x_6x_9 \oplus x_0x_1x_3x_7 \oplus x_0x_1x_3x_7x_8 \oplus x_0x_1x_3x_7x_8x_9 \oplus x_0x_1x_3x_8x_9 \oplus x_0x_1x_3x_9 \oplus x_0x_1x_4 \oplus$$
$$x_0x_1x_4x_5x_6\oplus x_0x_1x_4x_5x_6x_7x_8\oplus x_0x_1x_4x_5x_6x_7x_9\oplus x_0x_1x_4x_5x_6x_8\oplus x_0x_1x_4x_5x_6x_8x_9\oplus x_0x_1x_4x_5x_7\oplus x_0x_1x_4x_5x_7x_8x_9\oplus$$
$$x_0x_1x_4x_5x_7x_9 \oplus x_0x_1x_4x_5x_8 \oplus x_0x_1x_4x_5x_9 \oplus x_0x_1x_4x_6 \oplus x_0x_1x_4x_6x_7 \oplus x_0x_1x_4x_6x_7x_8 \oplus x_0x_1x_4x_6x_7x_8x_9 \oplus$$
$$x_0x_1x_4x_6x_8x_9 \oplus x_0x_1x_4x_6x_9 \oplus x_0x_1x_4x_7x_8 \oplus x_0x_1x_4x_7x_9 \oplus x_0x_1x_4x_8 \oplus x_0x_1x_4x_8x_9 \oplus x_0x_1x_5 \oplus x_0x_1x_5x_6x_7 \oplus$$
$$x_0x_1x_5x_6x_7x_8x_9 \oplus x_0x_1x_5x_6x_7x_9 \oplus x_0x_1x_5x_6x_8 \oplus x_0x_1x_5x_6x_9 \oplus x_0x_1x_5x_7 \oplus x_0x_1x_5x_7x_8 \oplus x_0x_1x_5x_7x_8x_9 \oplus$$
$$x_0x_1x_5x_8x_9\oplus x_0x_1x_5x_9\oplus x_0x_1x_6\oplus x_0x_1x_6x_7x_8\oplus x_0x_1x_6x_7x_9\oplus x_0x_1x_6x_8\oplus x_0x_1x_6x_8x_9\oplus x_0x_1x_7\oplus x_0x_1x_7x_8x_9\oplus$$
$$x_0x_1x_7x_9 \oplus x_0x_1x_8 \oplus x_0x_1x_9 \oplus x_0x_2 \oplus x_0x_2x_3 \oplus x_0x_2x_3x_4 \oplus x_0x_2x_3x_4x_5 \oplus x_0x_2x_3x_4x_5x_6 \oplus x_0x_2x_3x_4x_5x_6x_7 \oplus$$
$$x_0x_2x_3x_4x_5x_6x_7x_8\oplus x_0x_2x_3x_4x_5x_6x_7x_8x_9\oplus x_0x_2x_3x_4x_5x_6x_8x_9\oplus x_0x_2x_3x_4x_5x_6x_9\oplus x_0x_2x_3x_4x_5x_7x_8\oplus x_0x_2x_3x_4x_5x_7x_9\oplus$$
$$x_0x_2x_3x_4x_5x_8 \oplus x_0x_2x_3x_4x_5x_8x_9 \oplus x_0x_2x_3x_4x_6x_7 \oplus x_0x_2x_3x_4x_6x_7x_8x_9 \oplus x_0x_2x_3x_4x_6x_7x_9 \oplus x_0x_2x_3x_4x_6x_8 \oplus$$
$$x_0x_2x_3x_4x_6x_9\oplus x_0x_2x_3x_4x_7\oplus x_0x_2x_3x_4x_7x_8\oplus x_0x_2x_3x_4x_7x_8x_9\oplus x_0x_2x_3x_4x_8x_9\oplus x_0x_2x_3x_4x_9\oplus x_0x_2x_3x_5x_6\oplus$$
$$x_0x_2x_3x_5x_6x_7x_8 \oplus x_0x_2x_3x_5x_6x_7x_9 \oplus x_0x_2x_3x_5x_6x_8 \oplus x_0x_2x_3x_5x_6x_8x_9 \oplus x_0x_2x_3x_5x_7 \oplus x_0x_2x_3x_5x_7x_8x_9 \oplus$$
$$x_0x_2x_3x_5x_7x_9 \oplus x_0x_2x_3x_5x_8 \oplus x_0x_2x_3x_5x_9 \oplus x_0x_2x_3x_6 \oplus x_0x_2x_3x_6x_7 \oplus x_0x_2x_3x_6x_7x_8 \oplus x_0x_2x_3x_6x_7x_8x_9 \oplus$$
$$x_0x_2x_3x_6x_8x_9\oplus x_0x_2x_3x_6x_9\oplus x_0x_2x_3x_7x_8\oplus x_0x_2x_3x_7x_9\oplus x_0x_2x_3x_8\oplus x_0x_2x_3x_8x_9\oplus x_0x_2x_4x_5\oplus x_0x_2x_4x_5x_6x_7\oplus$$
$$x_0x_2x_4x_5x_6x_7x_8x_9 \oplus x_0x_2x_4x_5x_6x_7x_9 \oplus x_0x_2x_4x_5x_6x_8 \oplus x_0x_2x_4x_5x_6x_9 \oplus x_0x_2x_4x_5x_7 \oplus x_0x_2x_4x_5x_7x_8 \oplus$$
$$x_0x_2x_4x_5x_7x_8x_9 \oplus x_0x_2x_4x_5x_8x_9 \oplus x_0x_2x_4x_5x_9 \oplus x_0x_2x_4x_6 \oplus x_0x_2x_4x_6x_7x_8 \oplus x_0x_2x_4x_6x_7x_9 \oplus x_0x_2x_4x_6x_8 \oplus$$
$$x_0x_2x_4x_6x_8x_9 \oplus x_0x_2x_4x_7 \oplus x_0x_2x_4x_7x_8x_9 \oplus x_0x_2x_4x_7x_9 \oplus x_0x_2x_4x_8 \oplus x_0x_2x_4x_9 \oplus x_0x_2x_5 \oplus x_0x_2x_5x_6 \oplus$$
$$x_0x_2x_5x_6x_7 \oplus x_0x_2x_5x_6x_7x_8 \oplus x_0x_2x_5x_6x_7x_8x_9 \oplus x_0x_2x_5x_6x_8x_9 \oplus x_0x_2x_5x_6x_9 \oplus x_0x_2x_5x_7x_8 \oplus x_0x_2x_5x_7x_9 \oplus$$

$$x_0x_2x_5x_8 \oplus x_0x_2x_5x_8x_9 \oplus x_0x_2x_6x_7 \oplus x_0x_2x_6x_7x_8x_9 \oplus x_0x_2x_6x_7x_9 \oplus x_0x_2x_6x_8 \oplus x_0x_2x_6x_9 \oplus x_0x_2x_7 \oplus$$
$$x_0x_2x_7x_8 \oplus x_0x_2x_7x_8x_9 \oplus x_0x_2x_8x_9 \oplus x_0x_2x_9 \oplus x_0x_3x_4 \oplus x_0x_3x_4x_5x_6 \oplus x_0x_3x_4x_5x_6x_7x_8 \oplus x_0x_3x_4x_5x_6x_7x_9 \oplus$$
$$x_0x_3x_4x_5x_6x_8 \oplus x_0x_3x_4x_5x_6x_8x_9 \oplus x_0x_3x_4x_5x_7 \oplus x_0x_3x_4x_5x_7x_8x_9 \oplus x_0x_3x_4x_5x_7x_9 \oplus x_0x_3x_4x_5x_8 \oplus x_0x_3x_4x_5x_9 \oplus$$
$$x_0x_3x_4x_6 \oplus x_0x_3x_4x_6x_7 \oplus x_0x_3x_4x_6x_7x_8 \oplus x_0x_3x_4x_6x_7x_8x_9 \oplus x_0x_3x_4x_6x_8x_9 \oplus x_0x_3x_4x_6x_9 \oplus x_0x_3x_4x_7x_8 \oplus$$
$$x_0x_3x_4x_7x_9 \oplus x_0x_3x_4x_8 \oplus x_0x_3x_4x_8x_9 \oplus x_0x_3x_5 \oplus x_0x_3x_5x_6x_7 \oplus x_0x_3x_5x_6x_7x_8x_9 \oplus x_0x_3x_5x_6x_7x_9 \oplus x_0x_3x_5x_6x_8 \oplus$$
$$x_0x_3x_5x_6x_9 \oplus x_0x_3x_5x_7 \oplus x_0x_3x_5x_7x_8 \oplus x_0x_3x_5x_7x_8x_9 \oplus x_0x_3x_5x_8x_9 \oplus x_0x_3x_5x_9 \oplus x_0x_3x_6 \oplus x_0x_3x_6x_7x_8 \oplus$$
$$x_0x_3x_6x_7x_9 \oplus x_0x_3x_6x_8 \oplus x_0x_3x_6x_8x_9 \oplus x_0x_3x_7 \oplus x_0x_3x_7x_8x_9 \oplus x_0x_3x_7x_9 \oplus x_0x_3x_8 \oplus x_0x_3x_9 \oplus x_0x_4 \oplus x_0x_4x_5 \oplus$$
$$x_0x_4x_5x_6 \oplus x_0x_4x_5x_6x_7 \oplus x_0x_4x_5x_6x_7x_8 \oplus x_0x_4x_5x_6x_7x_8x_9 \oplus x_0x_4x_5x_6x_8x_9 \oplus x_0x_4x_5x_6x_9 \oplus x_0x_4x_5x_7x_8 \oplus$$
$$x_0x_4x_5x_7x_9 \oplus x_0x_4x_5x_8 \oplus x_0x_4x_5x_8x_9 \oplus x_0x_4x_6x_7 \oplus x_0x_4x_6x_7x_8x_9 \oplus x_0x_4x_6x_7x_9 \oplus x_0x_4x_6x_8 \oplus x_0x_4x_6x_9 \oplus$$
$$x_0x_4x_7 \oplus x_0x_4x_7x_8 \oplus x_0x_4x_7x_8x_9 \oplus x_0x_4x_8x_9 \oplus x_0x_4x_9 \oplus x_0x_5x_6 \oplus x_0x_5x_6x_7x_8 \oplus x_0x_5x_6x_7x_9 \oplus x_0x_5x_6x_8 \oplus$$
$$x_0x_5x_6x_8x_9 \oplus x_0x_5x_7 \oplus x_0x_5x_7x_8x_9 \oplus x_0x_5x_7x_9 \oplus x_0x_5x_8 \oplus x_0x_5x_9 \oplus x_0x_6 \oplus x_0x_6x_7 \oplus x_0x_6x_7x_8 \oplus x_0x_6x_7x_8x_9 \oplus$$
$$x_0x_6x_8x_9 \oplus x_0x_6x_9 \oplus x_0x_7x_8 \oplus x_0x_7x_9 \oplus x_0x_8 \oplus x_0x_8x_9 \oplus x_1 \oplus x_1x_2x_3 \oplus x_1x_2x_3x_4x_5 \oplus x_1x_2x_3x_4x_5x_6x_7 \oplus$$
$$x_1x_2x_3x_4x_5x_6x_7x_8x_9 \oplus x_1x_2x_3x_4x_5x_6x_7x_9 \oplus x_1x_2x_3x_4x_5x_6x_8 \oplus x_1x_2x_3x_4x_5x_6x_9 \oplus x_1x_2x_3x_4x_5x_7 \oplus x_1x_2x_3x_4x_5x_7x_8 \oplus$$
$$x_1x_2x_3x_4x_5x_7x_8x_9 \oplus x_1x_2x_3x_4x_5x_8x_9 \oplus x_1x_2x_3x_4x_5x_9 \oplus x_1x_2x_3x_4x_6 \oplus x_1x_2x_3x_4x_6x_7x_8 \oplus x_1x_2x_3x_4x_6x_7x_9 \oplus$$
$$x_1x_2x_3x_4x_6x_8 \oplus x_1x_2x_3x_4x_6x_8x_9 \oplus x_1x_2x_3x_4x_7 \oplus x_1x_2x_3x_4x_7x_8x_9 \oplus x_1x_2x_3x_4x_7x_9 \oplus x_1x_2x_3x_4x_8 \oplus x_1x_2x_3x_4x_9 \oplus$$
$$x_1x_2x_3x_5 \oplus x_1x_2x_3x_5x_6 \oplus x_1x_2x_3x_5x_6x_7 \oplus x_1x_2x_3x_5x_6x_7x_8 \oplus x_1x_2x_3x_5x_6x_7x_8x_9 \oplus x_1x_2x_3x_5x_6x_8x_9 \oplus x_1x_2x_3x_5x_6x_9 \oplus$$
$$x_1x_2x_3x_5x_7x_8 \oplus x_1x_2x_3x_5x_7x_9 \oplus x_1x_2x_3x_5x_8 \oplus x_1x_2x_3x_5x_8x_9 \oplus x_1x_2x_3x_6x_7 \oplus x_1x_2x_3x_6x_7x_8x_9 \oplus x_1x_2x_3x_6x_7x_9 \oplus$$
$$x_1x_2x_3x_6x_8 \oplus x_1x_2x_3x_6x_9 \oplus x_1x_2x_3x_7 \oplus x_1x_2x_3x_7x_8 \oplus x_1x_2x_3x_7x_8x_9 \oplus x_1x_2x_3x_8x_9 \oplus x_1x_2x_3x_9 \oplus x_1x_2x_4 \oplus$$
$$x_1x_2x_4x_5x_6 \oplus x_1x_2x_4x_5x_6x_7x_8 \oplus x_1x_2x_4x_5x_6x_7x_9 \oplus x_1x_2x_4x_5x_6x_8 \oplus x_1x_2x_4x_5x_6x_8x_9 \oplus x_1x_2x_4x_5x_7 \oplus x_1x_2x_4x_5x_7x_8x_9 \oplus$$
$$x_1x_2x_4x_5x_7x_9 \oplus x_1x_2x_4x_5x_8 \oplus x_1x_2x_4x_5x_9 \oplus x_1x_2x_4x_6 \oplus x_1x_2x_4x_6x_7 \oplus x_1x_2x_4x_6x_7x_8 \oplus x_1x_2x_4x_6x_7x_8x_9 \oplus$$
$$x_1x_2x_4x_6x_8x_9 \oplus x_1x_2x_4x_6x_9 \oplus x_1x_2x_4x_7x_8 \oplus x_1x_2x_4x_7x_9 \oplus x_1x_2x_4x_8 \oplus x_1x_2x_4x_8x_9 \oplus x_1x_2x_5 \oplus x_1x_2x_5x_6x_7 \oplus$$
$$x_1x_2x_5x_6x_7x_8x_9 \oplus x_1x_2x_5x_6x_7x_9 \oplus x_1x_2x_5x_6x_8 \oplus x_1x_2x_5x_6x_9 \oplus x_1x_2x_5x_7 \oplus x_1x_2x_5x_7x_8 \oplus x_1x_2x_5x_7x_8x_9 \oplus$$
$$x_1x_2x_5x_8x_9 \oplus x_1x_2x_5x_9 \oplus x_1x_2x_6 \oplus x_1x_2x_6x_7x_8 \oplus x_1x_2x_6x_7x_9 \oplus x_1x_2x_6x_8 \oplus x_1x_2x_6x_8x_9 \oplus x_1x_2x_7 \oplus x_1x_2x_7x_8x_9 \oplus$$
$$x_1x_2x_7x_9 \oplus x_1x_2x_8 \oplus x_1x_2x_9 \oplus x_1x_3 \oplus x_1x_3x_4 \oplus x_1x_3x_4x_5 \oplus x_1x_3x_4x_5x_6 \oplus x_1x_3x_4x_5x_6x_7 \oplus x_1x_3x_4x_5x_6x_7x_8 \oplus$$
$$x_1x_3x_4x_5x_6x_7x_8x_9 \oplus x_1x_3x_4x_5x_6x_8x_9 \oplus x_1x_3x_4x_5x_6x_9 \oplus x_1x_3x_4x_5x_7x_8 \oplus x_1x_3x_4x_5x_7x_9 \oplus x_1x_3x_4x_5x_8 \oplus$$
$$x_1x_3x_4x_5x_8x_9 \oplus x_1x_3x_4x_6x_7 \oplus x_1x_3x_4x_6x_7x_8x_9 \oplus x_1x_3x_4x_6x_7x_9 \oplus x_1x_3x_4x_6x_8 \oplus x_1x_3x_4x_6x_9 \oplus x_1x_3x_4x_7 \oplus$$
$$x_1x_3x_4x_7x_8 \oplus x_1x_3x_4x_7x_8x_9 \oplus x_1x_3x_4x_8x_9 \oplus x_1x_3x_4x_9 \oplus x_1x_3x_5x_6 \oplus x_1x_3x_5x_6x_7x_8 \oplus x_1x_3x_5x_6x_7x_9 \oplus x_1x_3x_5x_6x_8 \oplus$$
$$x_1x_3x_5x_6x_8x_9 \oplus x_1x_3x_5x_7 \oplus x_1x_3x_5x_7x_8x_9 \oplus x_1x_3x_5x_7x_9 \oplus x_1x_3x_5x_8 \oplus x_1x_3x_5x_9 \oplus x_1x_3x_6 \oplus x_1x_3x_6x_7 \oplus$$
$$x_1x_3x_6x_7x_8 \oplus x_1x_3x_6x_7x_8x_9 \oplus x_1x_3x_6x_8x_9 \oplus x_1x_3x_6x_9 \oplus x_1x_3x_7x_8 \oplus x_1x_3x_7x_9 \oplus x_1x_3x_8 \oplus x_1x_3x_8x_9 \oplus x_1x_4x_5 \oplus$$
$$x_1x_4x_5x_6x_7 \oplus x_1x_4x_5x_6x_7x_8x_9 \oplus x_1x_4x_5x_6x_7x_9 \oplus x_1x_4x_5x_6x_8 \oplus x_1x_4x_5x_6x_9 \oplus x_1x_4x_5x_7 \oplus x_1x_4x_5x_7x_8 \oplus$$
$$x_1x_4x_5x_7x_8x_9 \oplus x_1x_4x_5x_8x_9 \oplus x_1x_4x_5x_9 \oplus x_1x_4x_6 \oplus x_1x_4x_6x_7x_8 \oplus x_1x_4x_6x_7x_9 \oplus x_1x_4x_6x_8 \oplus x_1x_4x_6x_8x_9 \oplus$$
$$x_1x_4x_7 \oplus x_1x_4x_7x_8x_9 \oplus x_1x_4x_7x_9 \oplus x_1x_4x_8 \oplus x_1x_4x_9 \oplus x_1x_5 \oplus x_1x_5x_6 \oplus x_1x_5x_6x_7 \oplus x_1x_5x_6x_7x_8 \oplus x_1x_5x_6x_7x_8x_9 \oplus$$
$$x_1x_5x_6x_8x_9 \oplus x_1x_5x_6x_9 \oplus x_1x_5x_7x_8 \oplus x_1x_5x_7x_9 \oplus x_1x_5x_8 \oplus x_1x_5x_8x_9 \oplus x_1x_6x_7 \oplus x_1x_6x_7x_8x_9 \oplus x_1x_6x_7x_9 \oplus$$
$$x_1x_6x_8 \oplus x_1x_6x_9 \oplus x_1x_7 \oplus x_1x_7x_8 \oplus x_1x_7x_8x_9 \oplus x_1x_8x_9 \oplus x_1x_9 \oplus x_2 \oplus x_2x_3x_4 \oplus x_2x_3x_4x_5x_6 \oplus x_2x_3x_4x_5x_6x_7x_8 \oplus$$
$$x_2x_3x_4x_5x_6x_7x_9 \oplus x_2x_3x_4x_5x_6x_8 \oplus x_2x_3x_4x_5x_6x_8x_9 \oplus x_2x_3x_4x_5x_7 \oplus x_2x_3x_4x_5x_7x_8x_9 \oplus x_2x_3x_4x_5x_7x_9 \oplus$$
$$x_2x_3x_4x_5x_8 \oplus x_2x_3x_4x_5x_9 \oplus x_2x_3x_4x_6 \oplus x_2x_3x_4x_6x_7 \oplus x_2x_3x_4x_6x_7x_8 \oplus x_2x_3x_4x_6x_7x_8x_9 \oplus x_2x_3x_4x_6x_8x_9 \oplus$$
$$x_2x_3x_4x_6x_9 \oplus x_2x_3x_4x_7x_8 \oplus x_2x_3x_4x_7x_9 \oplus x_2x_3x_4x_8 \oplus x_2x_3x_4x_8x_9 \oplus x_2x_3x_5 \oplus x_2x_3x_5x_6x_7 \oplus x_2x_3x_5x_6x_7x_8x_9 \oplus$$
$$x_2x_3x_5x_6x_7x_9 \oplus x_2x_3x_5x_6x_8 \oplus x_2x_3x_5x_6x_9 \oplus x_2x_3x_5x_7 \oplus x_2x_3x_5x_7x_8 \oplus x_2x_3x_5x_7x_8x_9 \oplus x_2x_3x_5x_8x_9 \oplus x_2x_3x_5x_9 \oplus$$
$$x_2x_3x_6 \oplus x_2x_3x_6x_7x_8 \oplus x_2x_3x_6x_7x_9 \oplus x_2x_3x_6x_8 \oplus x_2x_3x_6x_8x_9 \oplus x_2x_3x_7 \oplus x_2x_3x_7x_8x_9 \oplus x_2x_3x_7x_9 \oplus x_2x_3x_8 \oplus$$
$$x_2x_3x_9 \oplus x_2x_4 \oplus x_2x_4x_5 \oplus x_2x_4x_5x_6 \oplus x_2x_4x_5x_6x_7 \oplus x_2x_4x_5x_6x_7x_8 \oplus x_2x_4x_5x_6x_7x_8x_9 \oplus x_2x_4x_5x_6x_8x_9 \oplus$$
$$x_2x_4x_5x_6x_9 \oplus x_2x_4x_5x_7x_8 \oplus x_2x_4x_5x_7x_9 \oplus x_2x_4x_5x_8 \oplus x_2x_4x_5x_8x_9 \oplus x_2x_4x_6x_7 \oplus x_2x_4x_6x_7x_8x_9 \oplus x_2x_4x_6x_7x_9 \oplus$$
$$x_2x_4x_6x_8 \oplus x_2x_4x_6x_9 \oplus x_2x_4x_7 \oplus x_2x_4x_7x_8 \oplus x_2x_4x_7x_8x_9 \oplus x_2x_4x_8x_9 \oplus x_2x_4x_9 \oplus x_2x_5x_6 \oplus x_2x_5x_6x_7x_8 \oplus$$
$$x_2x_5x_6x_7x_9 \oplus x_2x_5x_6x_8 \oplus x_2x_5x_6x_8x_9 \oplus x_2x_5x_7 \oplus x_2x_5x_7x_8x_9 \oplus x_2x_5x_7x_9 \oplus x_2x_5x_8 \oplus x_2x_5x_9 \oplus x_2x_6 \oplus x_2x_6x_7 \oplus$$
$$x_2x_6x_7x_8 \oplus x_2x_6x_7x_8x_9 \oplus x_2x_6x_8x_9 \oplus x_2x_6x_9 \oplus x_2x_7x_8 \oplus x_2x_7x_9 \oplus x_2x_8 \oplus x_2x_8x_9 \oplus x_3 \oplus x_3x_4x_5 \oplus x_3x_4x_5x_6x_7 \oplus$$
$$x_3x_4x_5x_6x_7x_8x_9 \oplus x_3x_4x_5x_6x_7x_9 \oplus x_3x_4x_5x_6x_8 \oplus x_3x_4x_5x_6x_9 \oplus x_3x_4x_5x_7 \oplus x_3x_4x_5x_7x_8 \oplus x_3x_4x_5x_7x_8x_9 \oplus$$
$$x_3x_4x_5x_8x_9 \oplus x_3x_4x_5x_9 \oplus x_3x_4x_6 \oplus x_3x_4x_6x_7x_8 \oplus x_3x_4x_6x_7x_9 \oplus x_3x_4x_6x_8 \oplus x_3x_4x_6x_8x_9 \oplus x_3x_4x_7 \oplus x_3x_4x_7x_8x_9 \oplus$$
$$x_3x_4x_7x_9 \oplus x_3x_4x_8 \oplus x_3x_4x_9 \oplus x_3x_5 \oplus x_3x_5x_6 \oplus x_3x_5x_6x_7 \oplus x_3x_5x_6x_7x_8 \oplus x_3x_5x_6x_7x_8x_9 \oplus x_3x_5x_6x_8x_9 \oplus$$
$$x_3x_5x_6x_9 \oplus x_3x_5x_7x_8 \oplus x_3x_5x_7x_9 \oplus x_3x_5x_8 \oplus x_3x_5x_8x_9 \oplus x_3x_6x_7 \oplus x_3x_6x_7x_8x_9 \oplus x_3x_6x_7x_9 \oplus x_3x_6x_8 \oplus x_3x_6x_9 \oplus$$
$$x_3x_7 \oplus x_3x_7x_8 \oplus x_3x_7x_8x_9 \oplus x_3x_8x_9 \oplus x_3x_9 \oplus x_4 \oplus x_4x_5x_6 \oplus x_4x_5x_6x_7x_8 \oplus x_4x_5x_6x_7x_9 \oplus x_4x_5x_6x_8 \oplus x_4x_5x_6x_8x_9 \oplus$$
$$x_4x_5x_7 \oplus x_4x_5x_7x_8x_9 \oplus x_4x_5x_7x_9 \oplus x_4x_5x_8 \oplus x_4x_5x_9 \oplus x_4x_6 \oplus x_4x_6x_7 \oplus x_4x_6x_7x_8 \oplus x_4x_6x_7x_8x_9 \oplus x_4x_6x_8x_9 \oplus$$
$$x_4x_6x_9 \oplus x_4x_7x_8 \oplus x_4x_7x_9 \oplus x_4x_8 \oplus x_4x_8x_9 \oplus x_5 \oplus x_5x_6x_7 \oplus x_5x_6x_7x_8x_9 \oplus x_5x_6x_7x_9 \oplus x_5x_6x_8 \oplus x_5x_6x_9 \oplus x_5x_7 \oplus$$

$$x_5x_7x_8 \oplus x_5x_7x_8x_9 \oplus x_5x_8x_9 \oplus x_5x_9 \oplus x_6 \oplus x_6x_7x_8 \oplus x_6x_7x_9 \oplus x_6x_8 \oplus x_6x_8x_9 \oplus x_7 \oplus x_7x_8x_9 \oplus x_7x_9 \oplus x_8 \oplus x_9 = 1$$

$$x_0x_1 \oplus x_0x_1x_2x_3 \oplus x_0x_1x_2x_3x_4x_5 \oplus x_0x_1x_2x_3x_4x_5x_6x_7 \oplus x_0x_1x_2x_3x_4x_5x_6x_7x_8x_9 \oplus x_0x_1x_2x_3x_4x_5x_6x_7x_9 \oplus$$
$$x_0x_1x_2x_3x_4x_5x_6x_8 \oplus x_0x_1x_2x_3x_4x_5x_6x_9 \oplus x_0x_1x_2x_3x_4x_5x_7 \oplus x_0x_1x_2x_3x_4x_5x_7x_8 \oplus x_0x_1x_2x_3x_4x_5x_7x_8x_9 \oplus$$
$$x_0x_1x_2x_3x_4x_5x_8x_9 \oplus x_0x_1x_2x_3x_4x_5x_9 \oplus x_0x_1x_2x_3x_4x_6 \oplus x_0x_1x_2x_3x_4x_6x_7x_8 \oplus x_0x_1x_2x_3x_4x_6x_7x_9 \oplus x_0x_1x_2x_3x_4x_6x_8 \oplus$$
$$x_0x_1x_2x_3x_4x_6x_8x_9 \oplus x_0x_1x_2x_3x_4x_7 \oplus x_0x_1x_2x_3x_4x_7x_8x_9 \oplus x_0x_1x_2x_3x_4x_7x_9 \oplus x_0x_1x_2x_3x_4x_8 \oplus x_0x_1x_2x_3x_4x_9 \oplus$$
$$x_0x_1x_2x_3x_5 \oplus x_0x_1x_2x_3x_5x_6 \oplus x_0x_1x_2x_3x_5x_6x_7 \oplus x_0x_1x_2x_3x_5x_6x_7x_8 \oplus x_0x_1x_2x_3x_5x_6x_7x_8x_9 \oplus x_0x_1x_2x_3x_5x_6x_8x_9 \oplus$$
$$x_0x_1x_2x_3x_5x_6x_9 \oplus x_0x_1x_2x_3x_5x_7x_8 \oplus x_0x_1x_2x_3x_5x_7x_9 \oplus x_0x_1x_2x_3x_5x_8 \oplus x_0x_1x_2x_3x_5x_8x_9 \oplus x_0x_1x_2x_3x_6x_7 \oplus$$
$$x_0x_1x_2x_3x_6x_7x_8x_9 \oplus x_0x_1x_2x_3x_6x_7x_9 \oplus x_0x_1x_2x_3x_6x_8 \oplus x_0x_1x_2x_3x_6x_9 \oplus x_0x_1x_2x_3x_7 \oplus x_0x_1x_2x_3x_7x_8 \oplus$$
$$x_0x_1x_2x_3x_7x_8x_9 \oplus x_0x_1x_2x_3x_8x_9 \oplus x_0x_1x_2x_3x_9 \oplus x_0x_1x_2x_4 \oplus x_0x_1x_2x_4x_5x_6 \oplus x_0x_1x_2x_4x_5x_6x_7x_8 \oplus x_0x_1x_2x_4x_5x_6x_7x_9 \oplus$$
$$x_0x_1x_2x_4x_5x_6x_8 \oplus x_0x_1x_2x_4x_5x_6x_8x_9 \oplus x_0x_1x_2x_4x_5x_7 \oplus x_0x_1x_2x_4x_5x_7x_8x_9 \oplus x_0x_1x_2x_4x_5x_7x_9 \oplus x_0x_1x_2x_4x_5x_8 \oplus$$
$$x_0x_1x_2x_4x_5x_9 \oplus x_0x_1x_2x_4x_6 \oplus x_0x_1x_2x_4x_6x_7 \oplus x_0x_1x_2x_4x_6x_7x_8 \oplus x_0x_1x_2x_4x_6x_7x_8x_9 \oplus x_0x_1x_2x_4x_6x_8x_9 \oplus$$
$$x_0x_1x_2x_4x_6x_9 \oplus x_0x_1x_2x_4x_7x_8 \oplus x_0x_1x_2x_4x_7x_9 \oplus x_0x_1x_2x_4x_8 \oplus x_0x_1x_2x_4x_8x_9 \oplus x_0x_1x_2x_5 \oplus x_0x_1x_2x_5x_6x_7 \oplus$$
$$x_0x_1x_2x_5x_6x_7x_8x_9 \oplus x_0x_1x_2x_5x_6x_7x_9 \oplus x_0x_1x_2x_5x_6x_8 \oplus x_0x_1x_2x_5x_6x_9 \oplus x_0x_1x_2x_5x_7 \oplus x_0x_1x_2x_5x_7x_8 \oplus$$
$$x_0x_1x_2x_5x_7x_8x_9 \oplus x_0x_1x_2x_5x_8x_9 \oplus x_0x_1x_2x_5x_9 \oplus x_0x_1x_2x_6 \oplus x_0x_1x_2x_6x_7x_8 \oplus x_0x_1x_2x_6x_7x_9 \oplus x_0x_1x_2x_6x_8 \oplus$$
$$x_0x_1x_2x_6x_8x_9 \oplus x_0x_1x_2x_7 \oplus x_0x_1x_2x_7x_8x_9 \oplus x_0x_1x_2x_7x_9 \oplus x_0x_1x_2x_8 \oplus x_0x_1x_2x_9 \oplus x_0x_1x_3 \oplus x_0x_1x_3x_4 \oplus$$
$$x_0x_1x_3x_4x_5 \oplus x_0x_1x_3x_4x_5x_6 \oplus x_0x_1x_3x_4x_5x_6x_7 \oplus x_0x_1x_3x_4x_5x_6x_7x_8 \oplus x_0x_1x_3x_4x_5x_6x_7x_8x_9 \oplus x_0x_1x_3x_4x_5x_6x_8x_9 \oplus$$
$$x_0x_1x_3x_4x_5x_6x_9 \oplus x_0x_1x_3x_4x_5x_7x_8 \oplus x_0x_1x_3x_4x_5x_7x_9 \oplus x_0x_1x_3x_4x_5x_8 \oplus x_0x_1x_3x_4x_5x_8x_9 \oplus x_0x_1x_3x_4x_6x_7 \oplus$$
$$x_0x_1x_3x_4x_6x_7x_8x_9 \oplus x_0x_1x_3x_4x_6x_7x_9 \oplus x_0x_1x_3x_4x_6x_8 \oplus x_0x_1x_3x_4x_6x_9 \oplus x_0x_1x_3x_4x_7 \oplus x_0x_1x_3x_4x_7x_8 \oplus$$
$$x_0x_1x_3x_4x_7x_8x_9 \oplus x_0x_1x_3x_4x_8x_9 \oplus x_0x_1x_3x_4x_9 \oplus x_0x_1x_3x_5x_6 \oplus x_0x_1x_3x_5x_6x_7x_8 \oplus x_0x_1x_3x_5x_6x_7x_9 \oplus x_0x_1x_3x_5x_6x_8 \oplus$$
$$x_0x_1x_3x_5x_6x_8x_9 \oplus x_0x_1x_3x_5x_7 \oplus x_0x_1x_3x_5x_7x_8x_9 \oplus x_0x_1x_3x_5x_7x_9 \oplus x_0x_1x_3x_5x_8 \oplus x_0x_1x_3x_5x_9 \oplus x_0x_1x_3x_6 \oplus$$
$$x_0x_1x_3x_6x_7 \oplus x_0x_1x_3x_6x_7x_8 \oplus x_0x_1x_3x_6x_7x_8x_9 \oplus x_0x_1x_3x_6x_8x_9 \oplus x_0x_1x_3x_6x_9 \oplus x_0x_1x_3x_7x_8 \oplus x_0x_1x_3x_7x_9 \oplus$$
$$x_0x_1x_3x_8 \oplus x_0x_1x_3x_8x_9 \oplus x_0x_1x_4x_5 \oplus x_0x_1x_4x_5x_6x_7 \oplus x_0x_1x_4x_5x_6x_7x_8x_9 \oplus x_0x_1x_4x_5x_6x_7x_9 \oplus x_0x_1x_4x_5x_6x_8 \oplus$$
$$x_0x_1x_4x_5x_6x_9 \oplus x_0x_1x_4x_5x_7 \oplus x_0x_1x_4x_5x_7x_8 \oplus x_0x_1x_4x_5x_7x_8x_9 \oplus x_0x_1x_4x_5x_8x_9 \oplus x_0x_1x_4x_5x_9 \oplus x_0x_1x_4x_6 \oplus$$
$$x_0x_1x_4x_6x_7x_8 \oplus x_0x_1x_4x_6x_7x_9 \oplus x_0x_1x_4x_6x_8 \oplus x_0x_1x_4x_6x_8x_9 \oplus x_0x_1x_4x_7 \oplus x_0x_1x_4x_7x_8x_9 \oplus x_0x_1x_4x_7x_9 \oplus$$
$$x_0x_1x_4x_8 \oplus x_0x_1x_4x_9 \oplus x_0x_1x_5 \oplus x_0x_1x_5x_6 \oplus x_0x_1x_5x_6x_7 \oplus x_0x_1x_5x_6x_7x_8 \oplus x_0x_1x_5x_6x_7x_8x_9 \oplus x_0x_1x_5x_6x_8x_9 \oplus$$
$$x_0x_1x_5x_6x_9 \oplus x_0x_1x_5x_7x_8 \oplus x_0x_1x_5x_7x_9 \oplus x_0x_1x_5x_8 \oplus x_0x_1x_5x_8x_9 \oplus x_0x_1x_6x_7 \oplus x_0x_1x_6x_7x_8x_9 \oplus x_0x_1x_6x_7x_9 \oplus$$
$$x_0x_1x_6x_8 \oplus x_0x_1x_6x_9 \oplus x_0x_1x_7 \oplus x_0x_1x_7x_8 \oplus x_0x_1x_7x_8x_9 \oplus x_0x_1x_8x_9 \oplus x_0x_1x_9 \oplus x_0x_2 \oplus x_0x_2x_3x_4 \oplus x_0x_2x_3x_4x_5x_6 \oplus$$
$$x_0x_2x_3x_4x_5x_6x_7x_8 \oplus x_0x_2x_3x_4x_5x_6x_7x_9 \oplus x_0x_2x_3x_4x_5x_6x_8 \oplus x_0x_2x_3x_4x_5x_6x_8x_9 \oplus x_0x_2x_3x_4x_5x_7 \oplus x_0x_2x_3x_4x_5x_7x_8x_9 \oplus$$
$$x_0x_2x_3x_4x_5x_7x_9 \oplus x_0x_2x_3x_4x_5x_8 \oplus x_0x_2x_3x_4x_5x_9 \oplus x_0x_2x_3x_4x_6 \oplus x_0x_2x_3x_4x_6x_7 \oplus x_0x_2x_3x_4x_6x_7x_8 \oplus x_0x_2x_3x_4x_6x_7x_8x_9 \oplus$$
$$x_0x_2x_3x_4x_6x_8x_9 \oplus x_0x_2x_3x_4x_6x_9 \oplus x_0x_2x_3x_4x_7x_8 \oplus x_0x_2x_3x_4x_7x_9 \oplus x_0x_2x_3x_4x_8 \oplus x_0x_2x_3x_4x_8x_9 \oplus x_0x_2x_3x_5 \oplus$$
$$x_0x_2x_3x_5x_6x_7 \oplus x_0x_2x_3x_5x_6x_7x_8x_9 \oplus x_0x_2x_3x_5x_6x_7x_9 \oplus x_0x_2x_3x_5x_6x_8 \oplus x_0x_2x_3x_5x_6x_9 \oplus x_0x_2x_3x_5x_7 \oplus$$
$$x_0x_2x_3x_5x_7x_8 \oplus x_0x_2x_3x_5x_7x_8x_9 \oplus x_0x_2x_3x_5x_8x_9 \oplus x_0x_2x_3x_5x_9 \oplus x_0x_2x_3x_6 \oplus x_0x_2x_3x_6x_7x_8 \oplus x_0x_2x_3x_6x_7x_9 \oplus$$
$$x_0x_2x_3x_6x_8 \oplus x_0x_2x_3x_6x_8x_9 \oplus x_0x_2x_3x_7 \oplus x_0x_2x_3x_7x_8x_9 \oplus x_0x_2x_3x_7x_9 \oplus x_0x_2x_3x_8 \oplus x_0x_2x_3x_9 \oplus x_0x_2x_4 \oplus$$
$$x_0x_2x_4x_5 \oplus x_0x_2x_4x_5x_6 \oplus x_0x_2x_4x_5x_6x_7 \oplus x_0x_2x_4x_5x_6x_7x_8 \oplus x_0x_2x_4x_5x_6x_7x_8x_9 \oplus x_0x_2x_4x_5x_6x_8x_9 \oplus x_0x_2x_4x_5x_6x_9 \oplus$$
$$x_0x_2x_4x_5x_7x_8 \oplus x_0x_2x_4x_5x_7x_9 \oplus x_0x_2x_4x_5x_8 \oplus x_0x_2x_4x_5x_8x_9 \oplus x_0x_2x_4x_6x_7 \oplus x_0x_2x_4x_6x_7x_8x_9 \oplus x_0x_2x_4x_6x_7x_9 \oplus$$
$$x_0x_2x_4x_6x_8 \oplus x_0x_2x_4x_6x_9 \oplus x_0x_2x_4x_7 \oplus x_0x_2x_4x_7x_8 \oplus x_0x_2x_4x_7x_8x_9 \oplus x_0x_2x_4x_8x_9 \oplus x_0x_2x_4x_9 \oplus x_0x_2x_5x_6 \oplus$$
$$x_0x_2x_5x_6x_7x_8 \oplus x_0x_2x_5x_6x_7x_9 \oplus x_0x_2x_5x_6x_8 \oplus x_0x_2x_5x_6x_8x_9 \oplus x_0x_2x_5x_7 \oplus x_0x_2x_5x_7x_8x_9 \oplus x_0x_2x_5x_7x_9 \oplus$$
$$x_0x_2x_5x_8 \oplus x_0x_2x_5x_9 \oplus x_0x_2x_6 \oplus x_0x_2x_6x_7 \oplus x_0x_2x_6x_7x_8 \oplus x_0x_2x_6x_7x_8x_9 \oplus x_0x_2x_6x_8x_9 \oplus x_0x_2x_6x_9 \oplus x_0x_2x_7x_8 \oplus$$
$$x_0x_2x_7x_9 \oplus x_0x_2x_8 \oplus x_0x_2x_8x_9 \oplus x_0x_3 \oplus x_0x_3x_4x_5 \oplus x_0x_3x_4x_5x_6x_7 \oplus x_0x_3x_4x_5x_6x_7x_8x_9 \oplus x_0x_3x_4x_5x_6x_7x_9 \oplus$$
$$x_0x_3x_4x_5x_6x_8 \oplus x_0x_3x_4x_5x_6x_9 \oplus x_0x_3x_4x_5x_7 \oplus x_0x_3x_4x_5x_7x_8 \oplus x_0x_3x_4x_5x_7x_8x_9 \oplus x_0x_3x_4x_5x_8x_9 \oplus x_0x_3x_4x_5x_9 \oplus$$
$$x_0x_3x_4x_6 \oplus x_0x_3x_4x_6x_7x_8 \oplus x_0x_3x_4x_6x_7x_9 \oplus x_0x_3x_4x_6x_8 \oplus x_0x_3x_4x_6x_8x_9 \oplus x_0x_3x_4x_7 \oplus x_0x_3x_4x_7x_8x_9 \oplus$$
$$x_0x_3x_4x_7x_9 \oplus x_0x_3x_4x_8 \oplus x_0x_3x_4x_9 \oplus x_0x_3x_5 \oplus x_0x_3x_5x_6 \oplus x_0x_3x_5x_6x_7 \oplus x_0x_3x_5x_6x_7x_8 \oplus x_0x_3x_5x_6x_7x_8x_9 \oplus$$
$$x_0x_3x_5x_6x_8x_9 \oplus x_0x_3x_5x_6x_9 \oplus x_0x_3x_5x_7x_8 \oplus x_0x_3x_5x_7x_9 \oplus x_0x_3x_5x_8 \oplus x_0x_3x_5x_8x_9 \oplus x_0x_3x_6x_7 \oplus x_0x_3x_6x_7x_8x_9 \oplus$$
$$x_0x_3x_6x_7x_9 \oplus x_0x_3x_6x_8 \oplus x_0x_3x_6x_9 \oplus x_0x_3x_7 \oplus x_0x_3x_7x_8 \oplus x_0x_3x_7x_8x_9 \oplus x_0x_3x_8x_9 \oplus x_0x_3x_9 \oplus x_0x_4 \oplus x_0x_4x_5x_6 \oplus$$
$$x_0x_4x_5x_6x_7x_8 \oplus x_0x_4x_5x_6x_7x_9 \oplus x_0x_4x_5x_6x_8 \oplus x_0x_4x_5x_6x_8x_9 \oplus x_0x_4x_5x_7 \oplus x_0x_4x_5x_7x_8x_9 \oplus x_0x_4x_5x_7x_9 \oplus$$
$$x_0x_4x_5x_8 \oplus x_0x_4x_5x_9 \oplus x_0x_4x_6 \oplus x_0x_4x_6x_7 \oplus x_0x_4x_6x_7x_8 \oplus x_0x_4x_6x_7x_8x_9 \oplus x_0x_4x_6x_8x_9 \oplus x_0x_4x_6x_9 \oplus x_0x_4x_7x_8 \oplus$$
$$x_0x_4x_7x_9 \oplus x_0x_4x_8 \oplus x_0x_4x_8x_9 \oplus x_0x_5 \oplus x_0x_5x_6x_7 \oplus x_0x_5x_6x_7x_8x_9 \oplus x_0x_5x_6x_7x_9 \oplus x_0x_5x_6x_8 \oplus x_0x_5x_6x_9 \oplus$$
$$x_0x_5x_7 \oplus x_0x_5x_7x_8 \oplus x_0x_5x_7x_8x_9 \oplus x_0x_5x_8x_9 \oplus x_0x_5x_9 \oplus x_0x_6 \oplus x_0x_6x_7x_8 \oplus x_0x_6x_7x_9 \oplus x_0x_6x_8 \oplus x_0x_6x_8x_9 \oplus$$
$$x_0x_7 \oplus x_0x_7x_8x_9 \oplus x_0x_7x_9 \oplus x_0x_8 \oplus x_0x_9 \oplus x_1 \oplus x_1x_2 \oplus x_1x_2x_3 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_4x_5 \oplus x_1x_2x_3x_4x_5x_6 \oplus$$
$$x_1x_2x_3x_4x_5x_6x_7 \oplus x_1x_2x_3x_4x_5x_6x_7x_8 \oplus x_1x_2x_3x_4x_5x_6x_7x_8x_9 \oplus x_1x_2x_3x_4x_5x_6x_8x_9 \oplus x_1x_2x_3x_4x_5x_6x_9 \oplus x_1x_2x_3x_4x_5x_7x_8 \oplus$$
$$x_1x_2x_3x_4x_5x_7x_9 \oplus x_1x_2x_3x_4x_5x_8 \oplus x_1x_2x_3x_4x_5x_8x_9 \oplus x_1x_2x_3x_4x_6x_7 \oplus x_1x_2x_3x_4x_6x_7x_8x_9 \oplus x_1x_2x_3x_4x_6x_7x_9 \oplus$$

$$x_1x_2x_3x_4x_6x_8 \oplus x_1x_2x_3x_4x_6x_9 \oplus x_1x_2x_3x_4x_7 \oplus x_1x_2x_3x_4x_7x_8 \oplus x_1x_2x_3x_4x_7x_8x_9 \oplus x_1x_2x_3x_4x_8x_9 \oplus x_1x_2x_3x_4x_9 \oplus$$
$$x_1x_2x_3x_5x_6 \oplus x_1x_2x_3x_5x_6x_7x_8 \oplus x_1x_2x_3x_5x_6x_7x_9 \oplus x_1x_2x_3x_5x_6x_8 \oplus x_1x_2x_3x_5x_6x_8x_9 \oplus x_1x_2x_3x_5x_7 \oplus x_1x_2x_3x_5x_7x_8x_9 \oplus$$
$$x_1x_2x_3x_5x_7x_9 \oplus x_1x_2x_3x_5x_8 \oplus x_1x_2x_3x_5x_9 \oplus x_1x_2x_3x_6 \oplus x_1x_2x_3x_6x_7 \oplus x_1x_2x_3x_6x_7x_8 \oplus x_1x_2x_3x_6x_7x_8x_9 \oplus$$
$$x_1x_2x_3x_6x_8x_9 \oplus x_1x_2x_3x_6x_9 \oplus x_1x_2x_3x_7x_8 \oplus x_1x_2x_3x_7x_9 \oplus x_1x_2x_3x_8 \oplus x_1x_2x_3x_8x_9 \oplus x_1x_2x_4x_5 \oplus x_1x_2x_4x_5x_6x_7 \oplus$$
$$x_1x_2x_4x_5x_6x_7x_8x_9 \oplus x_1x_2x_4x_5x_6x_7x_9 \oplus x_1x_2x_4x_5x_6x_8 \oplus x_1x_2x_4x_5x_6x_9 \oplus x_1x_2x_4x_5x_7 \oplus x_1x_2x_4x_5x_7x_8 \oplus$$
$$x_1x_2x_4x_5x_7x_8x_9 \oplus x_1x_2x_4x_5x_8x_9 \oplus x_1x_2x_4x_5x_9 \oplus x_1x_2x_4x_6 \oplus x_1x_2x_4x_6x_7x_8 \oplus x_1x_2x_4x_6x_7x_9 \oplus x_1x_2x_4x_6x_8 \oplus$$
$$x_1x_2x_4x_6x_8x_9 \oplus x_1x_2x_4x_7 \oplus x_1x_2x_4x_7x_8x_9 \oplus x_1x_2x_4x_7x_9 \oplus x_1x_2x_4x_8 \oplus x_1x_2x_4x_9 \oplus x_1x_2x_5 \oplus x_1x_2x_5x_6 \oplus$$
$$x_1x_2x_5x_6x_7 \oplus x_1x_2x_5x_6x_7x_8 \oplus x_1x_2x_5x_6x_7x_8x_9 \oplus x_1x_2x_5x_6x_8x_9 \oplus x_1x_2x_5x_6x_9 \oplus x_1x_2x_5x_7x_8 \oplus x_1x_2x_5x_7x_9 \oplus$$
$$x_1x_2x_5x_8 \oplus x_1x_2x_5x_8x_9 \oplus x_1x_2x_6x_7 \oplus x_1x_2x_6x_7x_8x_9 \oplus x_1x_2x_6x_7x_9 \oplus x_1x_2x_6x_8 \oplus x_1x_2x_6x_9 \oplus x_1x_2x_7 \oplus$$
$$x_1x_2x_7x_8 \oplus x_1x_2x_7x_8x_9 \oplus x_1x_2x_8x_9 \oplus x_1x_2x_9 \oplus x_1x_3x_4 \oplus x_1x_3x_4x_5x_6 \oplus x_1x_3x_4x_5x_6x_7x_8 \oplus x_1x_3x_4x_5x_6x_7x_9 \oplus$$
$$x_1x_3x_4x_5x_6x_8 \oplus x_1x_3x_4x_5x_6x_8x_9 \oplus x_1x_3x_4x_5x_7 \oplus x_1x_3x_4x_5x_7x_8x_9 \oplus x_1x_3x_4x_5x_7x_9 \oplus x_1x_3x_4x_5x_8 \oplus x_1x_3x_4x_5x_9 \oplus$$
$$x_1x_3x_4x_6 \oplus x_1x_3x_4x_6x_7 \oplus x_1x_3x_4x_6x_7x_8 \oplus x_1x_3x_4x_6x_7x_8x_9 \oplus x_1x_3x_4x_6x_8x_9 \oplus x_1x_3x_4x_6x_9 \oplus x_1x_3x_4x_7x_8 \oplus$$
$$x_1x_3x_4x_7x_9 \oplus x_1x_3x_4x_8 \oplus x_1x_3x_4x_8x_9 \oplus x_1x_3x_5 \oplus x_1x_3x_5x_6x_7 \oplus x_1x_3x_5x_6x_7x_8x_9 \oplus x_1x_3x_5x_6x_7x_9 \oplus x_1x_3x_5x_6x_8 \oplus$$
$$x_1x_3x_5x_6x_9 \oplus x_1x_3x_5x_7 \oplus x_1x_3x_5x_7x_8 \oplus x_1x_3x_5x_7x_8x_9 \oplus x_1x_3x_5x_8x_9 \oplus x_1x_3x_5x_9 \oplus x_1x_3x_6 \oplus x_1x_3x_6x_7x_8 \oplus$$
$$x_1x_3x_6x_7x_9 \oplus x_1x_3x_6x_8 \oplus x_1x_3x_6x_8x_9 \oplus x_1x_3x_7 \oplus x_1x_3x_7x_8x_9 \oplus x_1x_3x_7x_9 \oplus x_1x_3x_8 \oplus x_1x_3x_9 \oplus x_1x_4 \oplus x_1x_4x_5 \oplus$$
$$x_1x_4x_5x_6 \oplus x_1x_4x_5x_6x_7 \oplus x_1x_4x_5x_6x_7x_8 \oplus x_1x_4x_5x_6x_7x_8x_9 \oplus x_1x_4x_5x_6x_8x_9 \oplus x_1x_4x_5x_6x_9 \oplus x_1x_4x_5x_7x_8 \oplus$$
$$x_1x_4x_5x_7x_9 \oplus x_1x_4x_5x_8 \oplus x_1x_4x_5x_8x_9 \oplus x_1x_4x_6x_7 \oplus x_1x_4x_6x_7x_8x_9 \oplus x_1x_4x_6x_7x_9 \oplus x_1x_4x_6x_8 \oplus x_1x_4x_6x_9 \oplus$$
$$x_1x_4x_7 \oplus x_1x_4x_7x_8 \oplus x_1x_4x_7x_8x_9 \oplus x_1x_4x_8x_9 \oplus x_1x_4x_9 \oplus x_1x_5x_6 \oplus x_1x_5x_6x_7x_8 \oplus x_1x_5x_6x_7x_9 \oplus x_1x_5x_6x_8 \oplus$$
$$x_1x_5x_6x_8x_9 \oplus x_1x_5x_7 \oplus x_1x_5x_7x_8x_9 \oplus x_1x_5x_7x_9 \oplus x_1x_5x_8 \oplus x_1x_5x_9 \oplus x_1x_6 \oplus x_1x_6x_7 \oplus x_1x_6x_7x_8 \oplus x_1x_6x_7x_8x_9 \oplus$$
$$x_1x_6x_8x_9 \oplus x_1x_6x_9 \oplus x_1x_7x_8 \oplus x_1x_7x_9 \oplus x_1x_8 \oplus x_1x_8x_9 \oplus x_2x_3 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_4x_5x_6x_7 \oplus x_2x_3x_4x_5x_6x_7x_8x_9 \oplus$$
$$x_2x_3x_4x_5x_6x_7x_9 \oplus x_2x_3x_4x_5x_6x_8 \oplus x_2x_3x_4x_5x_6x_9 \oplus x_2x_3x_4x_5x_7 \oplus x_2x_3x_4x_5x_7x_8 \oplus x_2x_3x_4x_5x_7x_8x_9 \oplus x_2x_3x_4x_5x_8x_9 \oplus$$
$$x_2x_3x_4x_5x_9 \oplus x_2x_3x_4x_6 \oplus x_2x_3x_4x_6x_7x_8 \oplus x_2x_3x_4x_6x_7x_9 \oplus x_2x_3x_4x_6x_8 \oplus x_2x_3x_4x_6x_8x_9 \oplus x_2x_3x_4x_7 \oplus x_2x_3x_4x_7x_8x_9 \oplus$$
$$x_2x_3x_4x_7x_9 \oplus x_2x_3x_4x_8 \oplus x_2x_3x_4x_9 \oplus x_2x_3x_5 \oplus x_2x_3x_5x_6 \oplus x_2x_3x_5x_6x_7 \oplus x_2x_3x_5x_6x_7x_8 \oplus x_2x_3x_5x_6x_7x_8x_9 \oplus$$
$$x_2x_3x_5x_6x_8x_9 \oplus x_2x_3x_5x_6x_9 \oplus x_2x_3x_5x_7x_8 \oplus x_2x_3x_5x_7x_9 \oplus x_2x_3x_5x_8 \oplus x_2x_3x_5x_8x_9 \oplus x_2x_3x_6x_7 \oplus x_2x_3x_6x_7x_8x_9 \oplus$$
$$x_2x_3x_6x_7x_9 \oplus x_2x_3x_6x_8 \oplus x_2x_3x_6x_9 \oplus x_2x_3x_7 \oplus x_2x_3x_7x_8 \oplus x_2x_3x_7x_8x_9 \oplus x_2x_3x_8x_9 \oplus x_2x_3x_9 \oplus x_2x_4 \oplus x_2x_4x_5x_6 \oplus$$
$$x_2x_4x_5x_6x_7x_8 \oplus x_2x_4x_5x_6x_7x_9 \oplus x_2x_4x_5x_6x_8 \oplus x_2x_4x_5x_6x_8x_9 \oplus x_2x_4x_5x_7 \oplus x_2x_4x_5x_7x_8x_9 \oplus x_2x_4x_5x_7x_9 \oplus$$
$$x_2x_4x_5x_8 \oplus x_2x_4x_5x_9 \oplus x_2x_4x_6 \oplus x_2x_4x_6x_7 \oplus x_2x_4x_6x_7x_8 \oplus x_2x_4x_6x_7x_8x_9 \oplus x_2x_4x_6x_8x_9 \oplus x_2x_4x_6x_9 \oplus x_2x_4x_7x_8 \oplus$$
$$x_2x_4x_7x_9 \oplus x_2x_4x_8 \oplus x_2x_4x_8x_9 \oplus x_2x_5 \oplus x_2x_5x_6x_7 \oplus x_2x_5x_6x_7x_8x_9 \oplus x_2x_5x_6x_7x_9 \oplus x_2x_5x_6x_8 \oplus x_2x_5x_6x_9 \oplus$$
$$x_2x_5x_7 \oplus x_2x_5x_7x_8 \oplus x_2x_5x_7x_8x_9 \oplus x_2x_5x_8x_9 \oplus x_2x_5x_9 \oplus x_2x_6 \oplus x_2x_6x_7x_8 \oplus x_2x_6x_7x_9 \oplus x_2x_6x_8 \oplus x_2x_6x_8x_9 \oplus$$
$$x_2x_7 \oplus x_2x_7x_8x_9 \oplus x_2x_7x_9 \oplus x_2x_8 \oplus x_2x_9 \oplus x_3 \oplus x_3x_4 \oplus x_3x_4x_5 \oplus x_3x_4x_5x_6 \oplus x_3x_4x_5x_6x_7 \oplus x_3x_4x_5x_6x_7x_8 \oplus$$
$$x_3x_4x_5x_6x_7x_8x_9 \oplus x_3x_4x_5x_6x_8x_9 \oplus x_3x_4x_5x_6x_9 \oplus x_3x_4x_5x_7x_8 \oplus x_3x_4x_5x_7x_9 \oplus x_3x_4x_5x_8 \oplus x_3x_4x_5x_8x_9 \oplus$$
$$x_3x_4x_6x_7 \oplus x_3x_4x_6x_7x_8x_9 \oplus x_3x_4x_6x_7x_9 \oplus x_3x_4x_6x_8 \oplus x_3x_4x_6x_9 \oplus x_3x_4x_7 \oplus x_3x_4x_7x_8 \oplus x_3x_4x_7x_8x_9 \oplus x_3x_4x_8x_9 \oplus$$
$$x_3x_4x_9 \oplus x_3x_5x_6 \oplus x_3x_5x_6x_7x_8 \oplus x_3x_5x_6x_7x_9 \oplus x_3x_5x_6x_8 \oplus x_3x_5x_6x_8x_9 \oplus x_3x_5x_7 \oplus x_3x_5x_7x_8x_9 \oplus x_3x_5x_7x_9 \oplus$$
$$x_3x_5x_8 \oplus x_3x_5x_9 \oplus x_3x_6 \oplus x_3x_6x_7 \oplus x_3x_6x_7x_8 \oplus x_3x_6x_7x_8x_9 \oplus x_3x_6x_8x_9 \oplus x_3x_6x_9 \oplus x_3x_7x_8 \oplus x_3x_7x_9 \oplus x_3x_8 \oplus$$
$$x_3x_8x_9 \oplus x_4x_5 \oplus x_4x_5x_6x_7 \oplus x_4x_5x_6x_7x_8x_9 \oplus x_4x_5x_6x_7x_9 \oplus x_4x_5x_6x_8 \oplus x_4x_5x_6x_9 \oplus x_4x_5x_7 \oplus x_4x_5x_7x_8 \oplus$$
$$x_4x_5x_7x_8x_9 \oplus x_4x_5x_8x_9 \oplus x_4x_5x_9 \oplus x_4x_6 \oplus x_4x_6x_7x_8 \oplus x_4x_6x_7x_9 \oplus x_4x_6x_8 \oplus x_4x_6x_8x_9 \oplus x_4x_7 \oplus x_4x_7x_8x_9 \oplus$$
$$x_4x_7x_9 \oplus x_4x_8 \oplus x_4x_9 \oplus x_5 \oplus x_5x_6 \oplus x_5x_6x_7 \oplus x_5x_6x_7x_8 \oplus x_5x_6x_7x_8x_9 \oplus x_5x_6x_8x_9 \oplus x_5x_6x_9 \oplus x_5x_7x_8 \oplus$$
$$x_5x_7x_9 \oplus x_5x_8 \oplus x_5x_8x_9 \oplus x_6x_7 \oplus x_6x_7x_8x_9 \oplus x_6x_7x_9 \oplus x_6x_8 \oplus x_6x_9 \oplus x_7 \oplus x_7x_8 \oplus x_7x_8x_9 \oplus x_8x_9 \oplus x_9 = 0$$

$$x_0 \oplus x_0x_1 \oplus x_0x_1x_2 \oplus x_0x_1x_2x_3 \oplus x_0x_1x_2x_3x_4 \oplus x_0x_1x_2x_3x_4x_5 \oplus x_0x_1x_2x_3x_4x_5x_6 \oplus x_0x_1x_2x_3x_4x_5x_6x_7 \oplus$$
$$x_0x_1x_2x_3x_4x_5x_6x_7x_8 \oplus x_0x_1x_2x_3x_4x_5x_6x_7x_8x_9 \oplus x_0x_1x_2x_3x_4x_5x_6x_8x_9 \oplus x_0x_1x_2x_3x_4x_5x_6x_9 \oplus x_0x_1x_2x_3x_4x_5x_7x_8 \oplus$$
$$x_0x_1x_2x_3x_4x_5x_7x_9 \oplus x_0x_1x_2x_3x_4x_5x_8 \oplus x_0x_1x_2x_3x_4x_5x_8x_9 \oplus x_0x_1x_2x_3x_4x_6x_7 \oplus x_0x_1x_2x_3x_4x_6x_7x_8x_9 \oplus x_0x_1x_2x_3x_4x_6x_7x_9 \oplus$$
$$x_0x_1x_2x_3x_4x_6x_8 \oplus x_0x_1x_2x_3x_4x_6x_9 \oplus x_0x_1x_2x_3x_4x_7 \oplus x_0x_1x_2x_3x_4x_7x_8 \oplus x_0x_1x_2x_3x_4x_7x_8x_9 \oplus x_0x_1x_2x_3x_4x_8x_9 \oplus$$
$$x_0x_1x_2x_3x_4x_9 \oplus x_0x_1x_2x_3x_5x_6 \oplus x_0x_1x_2x_3x_5x_6x_7x_8 \oplus x_0x_1x_2x_3x_5x_6x_7x_9 \oplus x_0x_1x_2x_3x_5x_6x_8 \oplus x_0x_1x_2x_3x_5x_6x_8x_9 \oplus$$
$$x_0x_1x_2x_3x_5x_7 \oplus x_0x_1x_2x_3x_5x_7x_8x_9 \oplus x_0x_1x_2x_3x_5x_7x_9 \oplus x_0x_1x_2x_3x_5x_8 \oplus x_0x_1x_2x_3x_5x_9 \oplus x_0x_1x_2x_3x_6 \oplus$$
$$x_0x_1x_2x_3x_6x_7 \oplus x_0x_1x_2x_3x_6x_7x_8 \oplus x_0x_1x_2x_3x_6x_7x_8x_9 \oplus x_0x_1x_2x_3x_6x_8x_9 \oplus x_0x_1x_2x_3x_6x_9 \oplus x_0x_1x_2x_3x_7x_8 \oplus$$
$$x_0x_1x_2x_3x_7x_9 \oplus x_0x_1x_2x_3x_8 \oplus x_0x_1x_2x_3x_8x_9 \oplus x_0x_1x_2x_4x_5 \oplus x_0x_1x_2x_4x_5x_6x_7 \oplus x_0x_1x_2x_4x_5x_6x_7x_8x_9 \oplus$$
$$x_0x_1x_2x_4x_5x_6x_7x_9 \oplus x_0x_1x_2x_4x_5x_6x_8 \oplus x_0x_1x_2x_4x_5x_6x_9 \oplus x_0x_1x_2x_4x_5x_7 \oplus x_0x_1x_2x_4x_5x_7x_8 \oplus x_0x_1x_2x_4x_5x_7x_8x_9 \oplus$$
$$x_0x_1x_2x_4x_5x_8x_9 \oplus x_0x_1x_2x_4x_5x_9 \oplus x_0x_1x_2x_4x_6 \oplus x_0x_1x_2x_4x_6x_7x_8 \oplus x_0x_1x_2x_4x_6x_7x_9 \oplus x_0x_1x_2x_4x_6x_8 \oplus$$
$$x_0x_1x_2x_4x_6x_8x_9 \oplus x_0x_1x_2x_4x_7 \oplus x_0x_1x_2x_4x_7x_8x_9 \oplus x_0x_1x_2x_4x_7x_9 \oplus x_0x_1x_2x_4x_8 \oplus x_0x_1x_2x_4x_9 \oplus x_0x_1x_2x_5 \oplus$$
$$x_0x_1x_2x_5x_6 \oplus x_0x_1x_2x_5x_6x_7 \oplus x_0x_1x_2x_5x_6x_7x_8 \oplus x_0x_1x_2x_5x_6x_7x_8x_9 \oplus x_0x_1x_2x_5x_6x_8x_9 \oplus x_0x_1x_2x_5x_6x_9 \oplus$$
$$x_0x_1x_2x_5x_7x_8 \oplus x_0x_1x_2x_5x_7x_9 \oplus x_0x_1x_2x_5x_8 \oplus x_0x_1x_2x_5x_8x_9 \oplus x_0x_1x_2x_6x_7 \oplus x_0x_1x_2x_6x_7x_8x_9 \oplus x_0x_1x_2x_6x_7x_9 \oplus$$

$$x_0x_1x_2x_6x_8 \oplus x_0x_1x_2x_6x_9 \oplus x_0x_1x_2x_7 \oplus x_0x_1x_2x_7x_8 \oplus x_0x_1x_2x_7x_8x_9 \oplus x_0x_1x_2x_8x_9 \oplus x_0x_1x_2x_9 \oplus x_0x_1x_3x_4 \oplus$$
$$x_0x_1x_3x_4x_5x_6 \oplus x_0x_1x_3x_4x_5x_6x_7x_8 \oplus x_0x_1x_3x_4x_5x_6x_7x_9 \oplus x_0x_1x_3x_4x_5x_6x_8 \oplus x_0x_1x_3x_4x_5x_6x_8x_9 \oplus x_0x_1x_3x_4x_5x_7 \oplus$$
$$x_0x_1x_3x_4x_5x_7x_8x_9 \oplus x_0x_1x_3x_4x_5x_7x_9 \oplus x_0x_1x_3x_4x_5x_8 \oplus x_0x_1x_3x_4x_5x_9 \oplus x_0x_1x_3x_4x_6 \oplus x_0x_1x_3x_4x_6x_7 \oplus$$
$$x_0x_1x_3x_4x_6x_7x_8 \oplus x_0x_1x_3x_4x_6x_7x_8x_9 \oplus x_0x_1x_3x_4x_6x_8x_9 \oplus x_0x_1x_3x_4x_6x_9 \oplus x_0x_1x_3x_4x_7x_8 \oplus x_0x_1x_3x_4x_7x_9 \oplus$$
$$x_0x_1x_3x_4x_8 \oplus x_0x_1x_3x_4x_8x_9 \oplus x_0x_1x_3x_5 \oplus x_0x_1x_3x_5x_6x_7 \oplus x_0x_1x_3x_5x_6x_7x_8x_9 \oplus x_0x_1x_3x_5x_6x_7x_9 \oplus x_0x_1x_3x_5x_6x_8 \oplus$$
$$x_0x_1x_3x_5x_6x_9 \oplus x_0x_1x_3x_5x_7 \oplus x_0x_1x_3x_5x_7x_8 \oplus x_0x_1x_3x_5x_7x_8x_9 \oplus x_0x_1x_3x_5x_8x_9 \oplus x_0x_1x_3x_5x_9 \oplus x_0x_1x_3x_6 \oplus$$
$$x_0x_1x_3x_6x_7x_8 \oplus x_0x_1x_3x_6x_7x_9 \oplus x_0x_1x_3x_6x_8 \oplus x_0x_1x_3x_6x_8x_9 \oplus x_0x_1x_3x_7 \oplus x_0x_1x_3x_7x_8x_9 \oplus x_0x_1x_3x_7x_9 \oplus$$
$$x_0x_1x_3x_8 \oplus x_0x_1x_3x_9 \oplus x_0x_1x_4 \oplus x_0x_1x_4x_5 \oplus x_0x_1x_4x_5x_6 \oplus x_0x_1x_4x_5x_6x_7 \oplus x_0x_1x_4x_5x_6x_7x_8 \oplus x_0x_1x_4x_5x_6x_7x_8x_9 \oplus$$
$$x_0x_1x_4x_5x_6x_8x_9 \oplus x_0x_1x_4x_5x_6x_9 \oplus x_0x_1x_4x_5x_7x_8 \oplus x_0x_1x_4x_5x_7x_9 \oplus x_0x_1x_4x_5x_8 \oplus x_0x_1x_4x_5x_8x_9 \oplus x_0x_1x_4x_6x_7 \oplus$$
$$x_0x_1x_4x_6x_7x_8x_9 \oplus x_0x_1x_4x_6x_7x_9 \oplus x_0x_1x_4x_6x_8 \oplus x_0x_1x_4x_6x_9 \oplus x_0x_1x_4x_7 \oplus x_0x_1x_4x_7x_8 \oplus x_0x_1x_4x_7x_8x_9 \oplus$$
$$x_0x_1x_4x_8x_9 \oplus x_0x_1x_4x_9 \oplus x_0x_1x_5x_6 \oplus x_0x_1x_5x_6x_7x_8 \oplus x_0x_1x_5x_6x_7x_9 \oplus x_0x_1x_5x_6x_8 \oplus x_0x_1x_5x_6x_8x_9 \oplus x_0x_1x_5x_7 \oplus$$
$$x_0x_1x_5x_7x_8x_9 \oplus x_0x_1x_5x_7x_9 \oplus x_0x_1x_5x_8 \oplus x_0x_1x_5x_9 \oplus x_0x_1x_6 \oplus x_0x_1x_6x_7 \oplus x_0x_1x_6x_7x_8 \oplus x_0x_1x_6x_7x_8x_9 \oplus$$
$$x_0x_1x_6x_8x_9 \oplus x_0x_1x_6x_9 \oplus x_0x_1x_7x_8 \oplus x_0x_1x_7x_9 \oplus x_0x_1x_8 \oplus x_0x_1x_8x_9 \oplus x_0x_2x_3 \oplus x_0x_2x_3x_4x_5 \oplus x_0x_2x_3x_4x_5x_6x_7 \oplus$$
$$x_0x_2x_3x_4x_5x_6x_7x_8x_9 \oplus x_0x_2x_3x_4x_5x_6x_7x_9 \oplus x_0x_2x_3x_4x_5x_6x_8 \oplus x_0x_2x_3x_4x_5x_6x_9 \oplus x_0x_2x_3x_4x_5x_7 \oplus x_0x_2x_3x_4x_5x_7x_8 \oplus$$
$$x_0x_2x_3x_4x_5x_7x_8x_9 \oplus x_0x_2x_3x_4x_5x_8x_9 \oplus x_0x_2x_3x_4x_5x_9 \oplus x_0x_2x_3x_4x_6 \oplus x_0x_2x_3x_4x_6x_7x_8 \oplus x_0x_2x_3x_4x_6x_7x_9 \oplus$$
$$x_0x_2x_3x_4x_6x_8 \oplus x_0x_2x_3x_4x_6x_8x_9 \oplus x_0x_2x_3x_4x_7 \oplus x_0x_2x_3x_4x_7x_8x_9 \oplus x_0x_2x_3x_4x_7x_9 \oplus x_0x_2x_3x_4x_8 \oplus x_0x_2x_3x_4x_9 \oplus$$
$$x_0x_2x_3x_5 \oplus x_0x_2x_3x_5x_6 \oplus x_0x_2x_3x_5x_6x_7 \oplus x_0x_2x_3x_5x_6x_7x_8 \oplus x_0x_2x_3x_5x_6x_7x_8x_9 \oplus x_0x_2x_3x_5x_6x_8x_9 \oplus x_0x_2x_3x_5x_6x_9 \oplus$$
$$x_0x_2x_3x_5x_7x_8 \oplus x_0x_2x_3x_5x_7x_9 \oplus x_0x_2x_3x_5x_8 \oplus x_0x_2x_3x_5x_8x_9 \oplus x_0x_2x_3x_6x_7 \oplus x_0x_2x_3x_6x_7x_8x_9 \oplus x_0x_2x_3x_6x_7x_9 \oplus$$
$$x_0x_2x_3x_6x_8 \oplus x_0x_2x_3x_6x_9 \oplus x_0x_2x_3x_7 \oplus x_0x_2x_3x_7x_8 \oplus x_0x_2x_3x_7x_8x_9 \oplus x_0x_2x_3x_8x_9 \oplus x_0x_2x_3x_9 \oplus x_0x_2x_4 \oplus$$
$$x_0x_2x_4x_5x_6 \oplus x_0x_2x_4x_5x_6x_7x_8 \oplus x_0x_2x_4x_5x_6x_7x_9 \oplus x_0x_2x_4x_5x_6x_8 \oplus x_0x_2x_4x_5x_6x_8x_9 \oplus x_0x_2x_4x_5x_7 \oplus x_0x_2x_4x_5x_7x_8x_9 \oplus$$
$$x_0x_2x_4x_5x_7x_9 \oplus x_0x_2x_4x_5x_8 \oplus x_0x_2x_4x_5x_9 \oplus x_0x_2x_4x_6 \oplus x_0x_2x_4x_6x_7 \oplus x_0x_2x_4x_6x_7x_8 \oplus x_0x_2x_4x_6x_7x_8x_9 \oplus$$
$$x_0x_2x_4x_6x_8x_9 \oplus x_0x_2x_4x_6x_9 \oplus x_0x_2x_4x_7x_8 \oplus x_0x_2x_4x_7x_9 \oplus x_0x_2x_4x_8 \oplus x_0x_2x_4x_8x_9 \oplus x_0x_2x_5 \oplus x_0x_2x_5x_6x_7 \oplus$$
$$x_0x_2x_5x_6x_7x_8x_9 \oplus x_0x_2x_5x_6x_7x_9 \oplus x_0x_2x_5x_6x_8 \oplus x_0x_2x_5x_6x_9 \oplus x_0x_2x_5x_7 \oplus x_0x_2x_5x_7x_8 \oplus x_0x_2x_5x_7x_8x_9 \oplus$$
$$x_0x_2x_5x_8x_9 \oplus x_0x_2x_5x_9 \oplus x_0x_2x_6 \oplus x_0x_2x_6x_7x_8 \oplus x_0x_2x_6x_7x_9 \oplus x_0x_2x_6x_8 \oplus x_0x_2x_6x_8x_9 \oplus x_0x_2x_7 \oplus x_0x_2x_7x_8x_9 \oplus$$
$$x_0x_2x_7x_9 \oplus x_0x_2x_8 \oplus x_0x_2x_9 \oplus x_0x_3 \oplus x_0x_3x_4 \oplus x_0x_3x_4x_5 \oplus x_0x_3x_4x_5x_6 \oplus x_0x_3x_4x_5x_6x_7 \oplus x_0x_3x_4x_5x_6x_7x_8 \oplus$$
$$x_0x_3x_4x_5x_6x_7x_8x_9 \oplus x_0x_3x_4x_5x_6x_8x_9 \oplus x_0x_3x_4x_5x_6x_9 \oplus x_0x_3x_4x_5x_7x_8 \oplus x_0x_3x_4x_5x_7x_9 \oplus x_0x_3x_4x_5x_8 \oplus$$
$$x_0x_3x_4x_5x_8x_9 \oplus x_0x_3x_4x_6x_7 \oplus x_0x_3x_4x_6x_7x_8x_9 \oplus x_0x_3x_4x_6x_7x_9 \oplus x_0x_3x_4x_6x_8 \oplus x_0x_3x_4x_6x_9 \oplus x_0x_3x_4x_7 \oplus$$
$$x_0x_3x_4x_7x_8 \oplus x_0x_3x_4x_7x_8x_9 \oplus x_0x_3x_4x_8x_9 \oplus x_0x_3x_4x_9 \oplus x_0x_3x_5x_6 \oplus x_0x_3x_5x_6x_7x_8 \oplus x_0x_3x_5x_6x_7x_9 \oplus x_0x_3x_5x_6x_8 \oplus$$
$$x_0x_3x_5x_6x_8x_9 \oplus x_0x_3x_5x_7 \oplus x_0x_3x_5x_7x_8x_9 \oplus x_0x_3x_5x_7x_9 \oplus x_0x_3x_5x_8 \oplus x_0x_3x_5x_9 \oplus x_0x_3x_6 \oplus x_0x_3x_6x_7 \oplus$$
$$x_0x_3x_6x_7x_8 \oplus x_0x_3x_6x_7x_8x_9 \oplus x_0x_3x_6x_8x_9 \oplus x_0x_3x_6x_9 \oplus x_0x_3x_7x_8 \oplus x_0x_3x_7x_9 \oplus x_0x_3x_8 \oplus x_0x_3x_8x_9 \oplus x_0x_4x_5 \oplus$$
$$x_0x_4x_5x_6x_7 \oplus x_0x_4x_5x_6x_7x_8x_9 \oplus x_0x_4x_5x_6x_7x_9 \oplus x_0x_4x_5x_6x_8 \oplus x_0x_4x_5x_6x_9 \oplus x_0x_4x_5x_7 \oplus x_0x_4x_5x_7x_8 \oplus$$
$$x_0x_4x_5x_7x_8x_9 \oplus x_0x_4x_5x_8x_9 \oplus x_0x_4x_5x_9 \oplus x_0x_4x_6 \oplus x_0x_4x_6x_7x_8 \oplus x_0x_4x_6x_7x_9 \oplus x_0x_4x_6x_8 \oplus x_0x_4x_6x_8x_9 \oplus$$
$$x_0x_4x_7 \oplus x_0x_4x_7x_8x_9 \oplus x_0x_4x_7x_9 \oplus x_0x_4x_8 \oplus x_0x_4x_9 \oplus x_0x_5 \oplus x_0x_5x_6 \oplus x_0x_5x_6x_7 \oplus x_0x_5x_6x_7x_8 \oplus x_0x_5x_6x_7x_8x_9 \oplus$$
$$x_0x_5x_6x_8x_9 \oplus x_0x_5x_6x_9 \oplus x_0x_5x_7x_8 \oplus x_0x_5x_7x_9 \oplus x_0x_5x_8 \oplus x_0x_5x_8x_9 \oplus x_0x_6x_7 \oplus x_0x_6x_7x_8x_9 \oplus x_0x_6x_7x_9 \oplus$$
$$x_0x_6x_8 \oplus x_0x_6x_9 \oplus x_0x_7 \oplus x_0x_7x_8 \oplus x_0x_7x_8x_9 \oplus x_0x_8x_9 \oplus x_0x_9 \oplus x_1x_2 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_4x_5x_6 \oplus$$
$$x_1x_2x_3x_4x_5x_6x_7x_8 \oplus x_1x_2x_3x_4x_5x_6x_7x_9 \oplus x_1x_2x_3x_4x_5x_6x_8 \oplus x_1x_2x_3x_4x_5x_6x_8x_9 \oplus x_1x_2x_3x_4x_5x_7 \oplus x_1x_2x_3x_4x_5x_7x_8x_9 \oplus$$
$$x_1x_2x_3x_4x_5x_7x_9 \oplus x_1x_2x_3x_4x_5x_8 \oplus x_1x_2x_3x_4x_5x_9 \oplus x_1x_2x_3x_4x_6 \oplus x_1x_2x_3x_4x_6x_7 \oplus x_1x_2x_3x_4x_6x_7x_8 \oplus x_1x_2x_3x_4x_6x_7x_8x_9 \oplus$$
$$x_1x_2x_3x_4x_6x_8x_9 \oplus x_1x_2x_3x_4x_6x_9 \oplus x_1x_2x_3x_4x_7x_8 \oplus x_1x_2x_3x_4x_7x_9 \oplus x_1x_2x_3x_4x_8 \oplus x_1x_2x_3x_4x_8x_9 \oplus x_1x_2x_3x_5 \oplus$$
$$x_1x_2x_3x_5x_6x_7 \oplus x_1x_2x_3x_5x_6x_7x_8x_9 \oplus x_1x_2x_3x_5x_6x_7x_9 \oplus x_1x_2x_3x_5x_6x_8 \oplus x_1x_2x_3x_5x_6x_9 \oplus x_1x_2x_3x_5x_7 \oplus$$
$$x_1x_2x_3x_5x_7x_8 \oplus x_1x_2x_3x_5x_7x_8x_9 \oplus x_1x_2x_3x_5x_8x_9 \oplus x_1x_2x_3x_5x_9 \oplus x_1x_2x_3x_6 \oplus x_1x_2x_3x_6x_7x_8 \oplus x_1x_2x_3x_6x_7x_9 \oplus$$
$$x_1x_2x_3x_6x_8 \oplus x_1x_2x_3x_6x_8x_9 \oplus x_1x_2x_3x_7 \oplus x_1x_2x_3x_7x_8x_9 \oplus x_1x_2x_3x_7x_9 \oplus x_1x_2x_3x_8 \oplus x_1x_2x_3x_9 \oplus x_1x_2x_4 \oplus$$
$$x_1x_2x_4x_5 \oplus x_1x_2x_4x_5x_6 \oplus x_1x_2x_4x_5x_6x_7 \oplus x_1x_2x_4x_5x_6x_7x_8 \oplus x_1x_2x_4x_5x_6x_7x_8x_9 \oplus x_1x_2x_4x_5x_6x_8x_9 \oplus x_1x_2x_4x_5x_6x_9 \oplus$$
$$x_1x_2x_4x_5x_7x_8 \oplus x_1x_2x_4x_5x_7x_9 \oplus x_1x_2x_4x_5x_8 \oplus x_1x_2x_4x_5x_8x_9 \oplus x_1x_2x_4x_6x_7 \oplus x_1x_2x_4x_6x_7x_8x_9 \oplus x_1x_2x_4x_6x_7x_9 \oplus$$
$$x_1x_2x_4x_6x_8 \oplus x_1x_2x_4x_6x_9 \oplus x_1x_2x_4x_7 \oplus x_1x_2x_4x_7x_8 \oplus x_1x_2x_4x_7x_8x_9 \oplus x_1x_2x_4x_8x_9 \oplus x_1x_2x_4x_9 \oplus x_1x_2x_5x_6 \oplus$$
$$x_1x_2x_5x_6x_7x_8 \oplus x_1x_2x_5x_6x_7x_9 \oplus x_1x_2x_5x_6x_8 \oplus x_1x_2x_5x_6x_8x_9 \oplus x_1x_2x_5x_7 \oplus x_1x_2x_5x_7x_8x_9 \oplus x_1x_2x_5x_7x_9 \oplus$$
$$x_1x_2x_5x_8 \oplus x_1x_2x_5x_9 \oplus x_1x_2x_6 \oplus x_1x_2x_6x_7 \oplus x_1x_2x_6x_7x_8 \oplus x_1x_2x_6x_7x_8x_9 \oplus x_1x_2x_6x_8x_9 \oplus x_1x_2x_6x_9 \oplus x_1x_2x_7x_8 \oplus$$
$$x_1x_2x_7x_9 \oplus x_1x_2x_8 \oplus x_1x_2x_8x_9 \oplus x_1x_3 \oplus x_1x_3x_4x_5 \oplus x_1x_3x_4x_5x_6x_7 \oplus x_1x_3x_4x_5x_6x_7x_8x_9 \oplus x_1x_3x_4x_5x_6x_7x_9 \oplus$$
$$x_1x_3x_4x_5x_6x_8 \oplus x_1x_3x_4x_5x_6x_9 \oplus x_1x_3x_4x_5x_7 \oplus x_1x_3x_4x_5x_7x_8 \oplus x_1x_3x_4x_5x_7x_8x_9 \oplus x_1x_3x_4x_5x_8x_9 \oplus x_1x_3x_4x_5x_9 \oplus$$
$$x_1x_3x_4x_6 \oplus x_1x_3x_4x_6x_7x_8 \oplus x_1x_3x_4x_6x_7x_9 \oplus x_1x_3x_4x_6x_8 \oplus x_1x_3x_4x_6x_8x_9 \oplus x_1x_3x_4x_7 \oplus x_1x_3x_4x_7x_8x_9 \oplus$$
$$x_1x_3x_4x_7x_9 \oplus x_1x_3x_4x_8 \oplus x_1x_3x_4x_9 \oplus x_1x_3x_5 \oplus x_1x_3x_5x_6 \oplus x_1x_3x_5x_6x_7 \oplus x_1x_3x_5x_6x_7x_8 \oplus x_1x_3x_5x_6x_7x_8x_9 \oplus$$
$$x_1x_3x_5x_6x_8x_9 \oplus x_1x_3x_5x_6x_9 \oplus x_1x_3x_5x_7x_8 \oplus x_1x_3x_5x_7x_9 \oplus x_1x_3x_5x_8 \oplus x_1x_3x_5x_8x_9 \oplus x_1x_3x_6x_7 \oplus x_1x_3x_6x_7x_8x_9 \oplus$$

$$x_1x_3x_6x_7x_9 \oplus x_1x_3x_6x_8 \oplus x_1x_3x_6x_9 \oplus x_1x_3x_7 \oplus x_1x_3x_7x_8 \oplus x_1x_3x_7x_8x_9 \oplus x_1x_3x_8x_9 \oplus x_1x_3x_9 \oplus x_1x_4 \oplus$$
$$x_1x_4x_5x_6 \oplus x_1x_4x_5x_6x_7x_8 \oplus x_1x_4x_5x_6x_7x_9 \oplus x_1x_4x_5x_6x_8 \oplus x_1x_4x_5x_6x_8x_9 \oplus x_1x_4x_5x_7 \oplus x_1x_4x_5x_7x_8x_9 \oplus$$
$$x_1x_4x_5x_7x_9 \oplus x_1x_4x_5x_8 \oplus x_1x_4x_5x_9 \oplus x_1x_4x_6 \oplus x_1x_4x_6x_7 \oplus x_1x_4x_6x_7x_8 \oplus x_1x_4x_6x_7x_8x_9 \oplus x_1x_4x_6x_8x_9 \oplus$$
$$x_1x_4x_6x_9 \oplus x_1x_4x_7x_8 \oplus x_1x_4x_7x_9 \oplus x_1x_4x_8 \oplus x_1x_4x_8x_9 \oplus x_1x_5 \oplus x_1x_5x_6x_7 \oplus x_1x_5x_6x_7x_8x_9 \oplus x_1x_5x_6x_7x_9 \oplus$$
$$x_1x_5x_6x_8 \oplus x_1x_5x_6x_9 \oplus x_1x_5x_7 \oplus x_1x_5x_7x_8 \oplus x_1x_5x_7x_8x_9 \oplus x_1x_5x_8x_9 \oplus x_1x_5x_9 \oplus x_1x_6 \oplus x_1x_6x_7x_8 \oplus x_1x_6x_7x_9 \oplus$$
$$x_1x_6x_8 \oplus x_1x_6x_8x_9 \oplus x_1x_7 \oplus x_1x_7x_8x_9 \oplus x_1x_7x_9 \oplus x_1x_8 \oplus x_1x_9 \oplus x_2 \oplus x_2x_3 \oplus x_2x_3x_4 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_4x_5x_6 \oplus$$
$$x_2x_3x_4x_5x_6x_7 \oplus x_2x_3x_4x_5x_6x_7x_8 \oplus x_2x_3x_4x_5x_6x_7x_8x_9 \oplus x_2x_3x_4x_5x_6x_8x_9 \oplus x_2x_3x_4x_5x_6x_9 \oplus x_2x_3x_4x_5x_7x_8 \oplus$$
$$x_2x_3x_4x_5x_7x_9 \oplus x_2x_3x_4x_5x_8 \oplus x_2x_3x_4x_5x_8x_9 \oplus x_2x_3x_4x_6x_7 \oplus x_2x_3x_4x_6x_7x_8x_9 \oplus x_2x_3x_4x_6x_7x_9 \oplus x_2x_3x_4x_6x_8 \oplus$$
$$x_2x_3x_4x_6x_9 \oplus x_2x_3x_4x_7 \oplus x_2x_3x_4x_7x_8 \oplus x_2x_3x_4x_7x_8x_9 \oplus x_2x_3x_4x_8x_9 \oplus x_2x_3x_4x_9 \oplus x_2x_3x_5x_6 \oplus x_2x_3x_5x_6x_7x_8 \oplus$$
$$x_2x_3x_5x_6x_7x_9 \oplus x_2x_3x_5x_6x_8 \oplus x_2x_3x_5x_6x_8x_9 \oplus x_2x_3x_5x_7 \oplus x_2x_3x_5x_7x_8x_9 \oplus x_2x_3x_5x_7x_9 \oplus x_2x_3x_5x_8 \oplus x_2x_3x_5x_9 \oplus$$
$$x_2x_3x_6 \oplus x_2x_3x_6x_7 \oplus x_2x_3x_6x_7x_8 \oplus x_2x_3x_6x_7x_8x_9 \oplus x_2x_3x_6x_8x_9 \oplus x_2x_3x_6x_9 \oplus x_2x_3x_7x_8 \oplus x_2x_3x_7x_9 \oplus$$
$$x_2x_3x_8 \oplus x_2x_3x_8x_9 \oplus x_2x_4x_5 \oplus x_2x_4x_5x_6x_7 \oplus x_2x_4x_5x_6x_7x_8x_9 \oplus x_2x_4x_5x_6x_7x_9 \oplus x_2x_4x_5x_6x_8 \oplus x_2x_4x_5x_6x_9 \oplus$$
$$x_2x_4x_5x_7 \oplus x_2x_4x_5x_7x_8 \oplus x_2x_4x_5x_7x_8x_9 \oplus x_2x_4x_5x_8x_9 \oplus x_2x_4x_5x_9 \oplus x_2x_4x_6 \oplus x_2x_4x_6x_7x_8 \oplus x_2x_4x_6x_7x_9 \oplus$$
$$x_2x_4x_6x_8 \oplus x_2x_4x_6x_8x_9 \oplus x_2x_4x_7 \oplus x_2x_4x_7x_8x_9 \oplus x_2x_4x_7x_9 \oplus x_2x_4x_8 \oplus x_2x_4x_9 \oplus x_2x_5 \oplus x_2x_5x_6 \oplus x_2x_5x_6x_7 \oplus$$
$$x_2x_5x_6x_7x_8 \oplus x_2x_5x_6x_7x_8x_9 \oplus x_2x_5x_6x_8x_9 \oplus x_2x_5x_6x_9 \oplus x_2x_5x_7x_8 \oplus x_2x_5x_7x_9 \oplus x_2x_5x_8 \oplus x_2x_5x_8x_9 \oplus x_2x_6x_7 \oplus$$
$$x_2x_6x_7x_8x_9 \oplus x_2x_6x_7x_9 \oplus x_2x_6x_8 \oplus x_2x_6x_9 \oplus x_2x_7 \oplus x_2x_7x_8 \oplus x_2x_7x_8x_9 \oplus x_2x_8x_9 \oplus x_2x_9 \oplus x_3x_4 \oplus x_3x_4x_5x_6 \oplus$$
$$x_3x_4x_5x_6x_7x_8 \oplus x_3x_4x_5x_6x_7x_9 \oplus x_3x_4x_5x_6x_8 \oplus x_3x_4x_5x_6x_8x_9 \oplus x_3x_4x_5x_7 \oplus x_3x_4x_5x_7x_8x_9 \oplus x_3x_4x_5x_7x_9 \oplus$$
$$x_3x_4x_5x_8 \oplus x_3x_4x_5x_9 \oplus x_3x_4x_6 \oplus x_3x_4x_6x_7 \oplus x_3x_4x_6x_7x_8 \oplus x_3x_4x_6x_7x_8x_9 \oplus x_3x_4x_6x_8x_9 \oplus x_3x_4x_6x_9 \oplus x_3x_4x_7x_8 \oplus$$
$$x_3x_4x_7x_9 \oplus x_3x_4x_8 \oplus x_3x_4x_8x_9 \oplus x_3x_5 \oplus x_3x_5x_6x_7 \oplus x_3x_5x_6x_7x_8x_9 \oplus x_3x_5x_6x_7x_9 \oplus x_3x_5x_6x_8 \oplus x_3x_5x_6x_9 \oplus$$
$$x_3x_5x_7 \oplus x_3x_5x_7x_8 \oplus x_3x_5x_7x_8x_9 \oplus x_3x_5x_8x_9 \oplus x_3x_5x_9 \oplus x_3x_6 \oplus x_3x_6x_7x_8 \oplus x_3x_6x_7x_9 \oplus x_3x_6x_8 \oplus x_3x_6x_8x_9 \oplus$$
$$x_3x_7 \oplus x_3x_7x_8x_9 \oplus x_3x_7x_9 \oplus x_3x_8 \oplus x_3x_9 \oplus x_4 \oplus x_4x_5 \oplus x_4x_5x_6 \oplus x_4x_5x_6x_7 \oplus x_4x_5x_6x_7x_8 \oplus x_4x_5x_6x_7x_8x_9 \oplus$$
$$x_4x_5x_6x_8x_9 \oplus x_4x_5x_6x_9 \oplus x_4x_5x_7x_8 \oplus x_4x_5x_7x_9 \oplus x_4x_5x_8 \oplus x_4x_5x_8x_9 \oplus x_4x_6x_7 \oplus x_4x_6x_7x_8x_9 \oplus x_4x_6x_7x_9 \oplus$$
$$x_4x_6x_8 \oplus x_4x_6x_9 \oplus x_4x_7 \oplus x_4x_7x_8 \oplus x_4x_7x_8x_9 \oplus x_4x_8x_9 \oplus x_4x_9 \oplus x_5x_6 \oplus x_5x_6x_7x_8 \oplus x_5x_6x_7x_9 \oplus x_5x_6x_8 \oplus$$
$$x_5x_6x_8x_9 \oplus x_5x_7 \oplus x_5x_7x_8x_9 \oplus x_5x_7x_9 \oplus x_5x_8 \oplus x_5x_9 \oplus x_6 \oplus x_6x_7 \oplus x_6x_7x_8 \oplus x_6x_7x_8x_9 \oplus x_6x_8x_9 \oplus x_6x_9 \oplus$$
$$x_7x_8 \oplus x_7x_9 \oplus x_8 \oplus x_8x_9 = 0$$

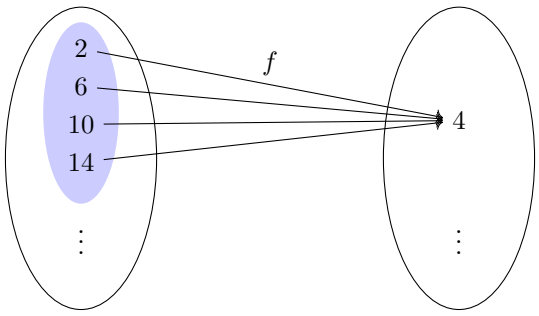
2 Retrodictive QFT

only need number of vars !!!!

solve other problems with just knowing which vars are involved

3 Alternative Introduction

Given finite sets A and B, a function $f : A \to B$ and an element $y \in B$, we define $\{\cdot \xleftarrow{f} y\}$, the pre-image of y under f, as the set $\{x \in A \mid f(x) = y\}$. For example, let $A = B = \{0, 1, \ldots, 15\}$ and let $f(x) = 7^x \mod 15$, then the collection of values that f maps to 4, $\{\cdot \xleftarrow{f} 4\}$, is the set $\{2, 6, 10, 14\}$.



Finding the pre-image of a function is a mathematical question that subsumes several practical computational problems such as pre-image attacks on hash functions [**10.1007/978-3-540-25937-4˙24**], predicting environmental conditions that allow certain reactions to take place in computational biology [**Klotz2013**,

akutsu2009analyses], and finding the pre-image of feature vectors in the space induced by a kernel in neural networks [**1353287**].

To appreciate the difficulty of computing pre-images in general, note that SAT is a boolean function over the input variables and that solving a SAT problem is asking for the pre-image of `true`. Indeed, based on the conjectured existence of one-way functions which itself implies $P \neq NP$, all these pre-images calculations are believed to be computationally intractable in their most general setting. What is however intriguing is that many computational problems that have efficient quantum algorithms are essentially queries over pre-images. We illustrate this connection briefly in the remainder of this section and analyze it further in the remainder of the paper.

Let $[\mathbf{n}]$ denote the finite set $\{0, 1, \ldots, (n-1)\}$. The parameter n determines the problem size in all the problems below (except Deutsch which is a fixed sized problem).

Deutsch. The conventional statement of the problem is to determine if a function $[\mathbf{2}] \rightarrow [\mathbf{2}]$ is constant or balanced. An equivalent statement is to answer a query about the cardinality of a pre-image. In this case, if the cardinality of the pre-image of any value in the range is even i.e. 0 or 2, the function must be constant and if it is odd, i.e., it contains just one element, the function must be balanced.

Deutsch-Jozsa. The problem is a generalization of the previous one: the question is to determine if a function $[\mathbf{2^n}] \rightarrow [\mathbf{2}]$ for some n is constant or balanced. When expressed as a pre-image computation, the problem reduces to a query distinguishing the following three situations about the pre-image of a value in the range of the function: is the cardinality of the pre-image equal to 0, 2^n, or 2^{n-1}? In the first two cases, the function is constant and in the last case, the pre-image contains half the values in the domain indicating that the function is balanced.

Bernstein-Vazirani. We are given a function $f : [\mathbf{2^n}] \rightarrow [\mathbf{2}]$ that hides a secret number $s \in [\mathbf{2^n}]$. We are promised the function is defined using the binary representations $\sum_i^{n-1} x_i$ and $\sum_i^{n-1} s_i$ of x and s respectively as follows:

$$f(x) = \sum_{i=0}^{n-1} s_i x_i \mod 2$$

The goal is to determine the secret number s.

Expressing the problem as a pre-image calculation is slightly more involved than in the previous two cases. To determine s, we make n queries to the pre-image of a value in the range of the function. Query i asks whether 2^i is a member of the pre-image and the answer determines bit i of the secret s. Indeed, by definition, $f(2^i) = s_i$ and hence s_i is 1 iff 2^i is a member of the pre-image of 1.

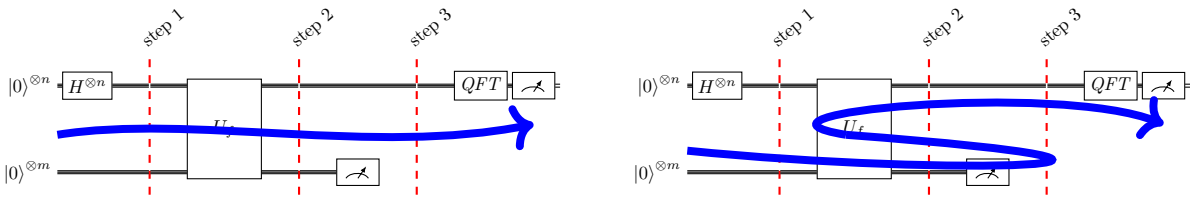
Simon. We are given a 2-1 function $f : [\mathbf{2^n}] \rightarrow [\mathbf{2^n}]$ with the property that there exists an a such $f(x) = f(x \oplus a)$ for all x; the goal is to determine a. When expressed as a computation of pre-images, the problem statement becomes the following. Pick an arbitrary x and compute the pre-image of $f(x)$. It must contain exactly two values one of which is x. The problem then reduces to finding the other value in the pre-image.

Shor. The quantum core of the algorithm is the following. We are given a periodic function $f(x) = a^x \mod 2^n$ and the goal is to determine the period. As a computation over pre-images, the problem can be recast as follows. For an arbitrary x, compute the pre-image of $f(x)$ and query it to determine the period.

core of many quantum algos is quantum oracle uf two inputs; two outputs system; ancilla; normal eval; control ancilla; system unknown; so throw in complete superposition and eval forward

how about if we look at ancilla (the one we control); look at one possible ancilla output; and go back (lazy) with partial information (symbolic pe); this realizes retrodictive!!!

The evolution of a quantum system is typically understood as proceeding forwards in time — from the present to the future. As shown in Fig. 5(a),



(a) Conventional Flow (b) Retrodictive Flow

Figure 6: Template quantum circuit

Since the conventional execution starts with complete ignorance about the future, the initial state is prepared as a superposition that includes every possibility. In a well-designed algorithm, , by the time the computation reaches the measurement stages, the relative phases and probability amplitudes in that enormous superposition have become biased towards states of interest which are projected to produce the final answer.

Retrodictive quantum theory [2], retrocausality [1], and the time-symmetry of physical laws [5] all suggest that partial knowledge about the future can be exploited to understand the present. This idea is demonstrated in Fig. 5(b) where the result of the measurement in the lower subsystem is used to retrodictively infer a sharper initial state which is then propagated forwards as usual. Surprisingly, we demonstrate that this idea allows us to *efficiently* realize some quantum algorithms by considering, exclusively, he classical fragment of the circuit (between steps 2 and 3) in Fig. 5.

Retrodictive:

Normal quantum evolution: from present to future

Now what if I had partial knowledge about the future; what can you say about the present? (And then about the rest of the unknown future)

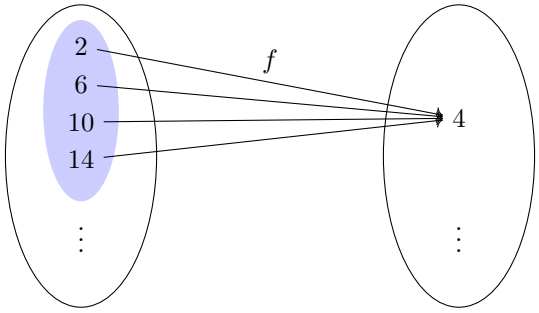
Can this help flow of information, complexity, etc?

In some cases, partial knowledge about the future is enough to predict the present accurately enough to then predict everything about the future; in some cases it is not enough

Possibility that collapse of wave function is information flow back from measured future to present unknown initial conditions and then back to rest of wave that was not measured

transactional interpretation?

Given finite sets A and B, a function $f : A \to B$ and an element $y \in B$, we define $\{\cdot \xleftarrow{f} y\}$, the pre-image of y under f, as the set $\{x \in A \mid f(x) = y\}$. For example, let $A = B = \{0, 1, \ldots, 15\}$ and let $f(x) = 7^x \mod 15$, then the collection of values that f maps to 4, $\{\cdot \xleftarrow{f} 4\}$, is the set $\{2, 6, 10, 14\}$.



Finding the pre-image of a function is a mathematical question that subsumes several practical computational problems such as pre-image attacks on hash functions [**10.1007/978-3-540-25937-4˙24**], predicting environmental conditions that allow certain reactions to take place in computational biology [**Klotz2013**, **akutsu2009analyses**], and finding the pre-image of feature vectors in the space induced by a kernel in neural networks [**1353287**].

To appreciate the difficulty of computing pre-images in general, note that SAT is a boolean function over the input variables and that solving a SAT problem is asking for the pre-image of `true`. Indeed, based on the conjectured existence of one-way functions which itself implies $P \neq NP$, all these pre-images calculations are believed to be computationally intractable in their most general setting. What is however intriguing is that many computational problems that have efficient quantum algorithms are essentially queries over pre-images. We illustrate this connection briefly in the remainder of this section and analyze it further in the remainder of the paper.

Let $[\mathbf{n}]$ denote the finite set $\{0, 1, \ldots, (n-1)\}$. The parameter n determines the problem size in all the problems below (except Deutsch which is a fixed sized problem).

Deutsch. The conventional statement of the problem is to determine if a function $[\mathbf{2}] \rightarrow [\mathbf{2}]$ is constant or balanced. An equivalent statement is to answer a query about the cardinality of a pre-image. In this case, if the cardinality of the pre-image of any value in the range is even i.e. 0 or 2, the function must be constant and if it is odd, i.e., it contains just one element, the function must be balanced.

Deutsch-Jozsa. The problem is a generalization of the previous one: the question is to determine if a function $[\mathbf{2^n}] \rightarrow [\mathbf{2}]$ for some n is constant or balanced. When expressed as a pre-image computation, the problem reduces to a query distinguishing the following three situations about the pre-image of a value in the range of the function: is the cardinality of the pre-image equal to 0, 2^n, or 2^{n-1}? In the first two cases, the function is constant and in the last case, the pre-image contains half the values in the domain indicating that the function is balanced.

Bernstein-Vazirani. We are given a function $f : [\mathbf{2^n}] \rightarrow [\mathbf{2}]$ that hides a secret number $s \in [\mathbf{2^n}]$. We are promised the function is defined using the binary representations $\sum_i^{n-1} x_i$ and $\sum_i^{n-1} s_i$ of x and s respectively as follows:

$$f(x) = \sum_{i=0}^{n-1} s_i x_i \mod 2$$

The goal is to determine the secret number s.

Expressing the problem as a pre-image calculation is slightly more involved than in the previous two cases. To determine s, we make n queries to the pre-image of a value in the range of the function. Query i asks whether 2^i is a member of the pre-image and the answer determines bit i of the secret s. Indeed, by definition, $f(2^i) = s_i$ and hence s_i is 1 iff 2^i is a member of the pre-image of 1.

Simon. We are given a 2-1 function $f : [\mathbf{2^n}] \rightarrow [\mathbf{2^n}]$ with the property that there exists an a such $f(x) = f(x \oplus a)$ for all x; the goal is to determine a. When expressed as a computation of pre-images, the problem statement becomes the following. Pick an arbitrary x and compute the pre-image of $f(x)$. It must contain exactly two values one of which is x. The problem then reduces to finding the other value in the pre-image.

Shor. The quantum core of the algorithm is the following. We are given a periodic function $f(x) = a^x \mod 2^n$ and the goal is to determine the period. As a computation over pre-images, the problem can be recast as follows. For an arbitrary x, compute the pre-image of $f(x)$ and query it to determine the period.

4 The Quantum Approach

A brute force solution to all the problems in the previous section is straightforward: try every value in the domain of the relevant function to calculate the required pre-image. Then, given complete knowledge of the pre-image, all the needed queries can be easily answered. This approach is, of course, not practical, as it is exponential in the problem size n. Furthermore, even if some shortcuts were discovered to speed up the

calculation of the pre-image, there is the additional non-trivial requirement of performing efficient queries on the pre-image.

Luckily, the problems of concern to us are quite special: (i) the functions are not arbitrary but have additional structure that can be exploited, and (ii) we never need access to all the elements in the pre-image; we just need to answer aggregate queries about the pre-images. Quantum algorithms somehow exploit these properties along with some physical principles to solve these problems efficiently. To understand the precise way in which this is happening, we start with the template of the quantum circuit used for solving all the problems above in Fig. 5.

The core of the circuit is the U_f block which can be assumed to be implemented using only generalized Toffoli gates. The block implements the unitary transformation: $U_f(|x\rangle\,|y\rangle) = |x\rangle\,|f(x) \oplus y\rangle$ where $\oplus$ is the (bitwise) exclusive-or operation; it defines the function of interest whose pre-image properties are to be calculated. The inputs of the U_f block are grouped in two registers: the top register contains an equal superposition of all possible inputs to f; the second register is prepared in initial states that depend on the specific algorithm. Thus, the state at slice (1) in the figure is:

$$\frac{1}{\sqrt{2^n}\sqrt{2^m}} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^m-1} |x\rangle\,|y\rangle$$

This is transformed by U_f to:

$$\frac{1}{\sqrt{2^n}\sqrt{2^m}} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^m-1} |x\rangle\,|f(x) \oplus y\rangle$$

So far, nothing too interesting is happening: we have just produced a superposition of states where each state is a possible input to f, say x, tensored with $f(x) \oplus y$, the result of applying f to this particular input adjusted by the second register y. At slice (3), something remarkable occurs; the result w of measuring the second register "kicks back" information to the first register whose state becomes a superposition of those values x that are consistent with the measurement, i.e., *the pre-image of w under f!* That pre-image representation is then analyzed using the Quantum Fourier Transform (QFT) to produce the final result.

To make the previous discussion more concrete, we show the full execution of the quantum algorithm on a few examples.

4.1 Bernstein-Vazirani

The circuit in Fig. 6 solves the problem for $n = 8$ and a hidden number 92 (= 00111010 in binary notation). As required, the circuit between slice (1) and slice (2), collects the sum of the x_i at positions that match the occurrences of 1 in the secret string. The evolution proceeds as follows. At slice (1), the top 8 qubits are each in the state $|+\rangle$ and the bottom qubit is in the state $|-\rangle$, i.e., the state is $(1/3)\ |+++++++++-\rangle$. In the evolution between slices (1) and (2), qubits 0, 2, 6, and 7 are untouched and remain in the state $|+\rangle$. Each of the other four qubits becomes $|-\rangle$ as the phase of the target qubit is kicked back to the control qubit by the CX operation. The full state at slice (2) is $(1/3)\ |+-+----++-\rangle$. At this point, we perform a measurement on the bottom qubit which returns 0 or 1 with equal probability. This measurement causes collapses the top 8 qubits to $\pm(1/2\sqrt{2})\ |+-+----++\rangle$. After applying all the Hadamard gates, the measurement is deterministically $|01011100\rangle$ with the most significant bit at the right. This is the secret number.

Instead of this execution model, we now explore an alternative execution that starts from the observation w and proceeds from slice (2) back towards slice (1) collecting the information necessary to answer the required pre-image query. As explained in the previous section, the secret number can be reconstructed once we know, for each i, whether the number 2^i is a member of the pre-image. When expressed in terms of bits, this means that we need to know, for each bit position i, whether the corresponding qubit contributes to the definition of the pre-image. We therefore start a backwards execution starting with the state $|x_0x_1x_2x_3x_4x_5x_6x_7F()\rangle$ where $F()$ expresses that the last qubit has not been shown to depend on any qubit

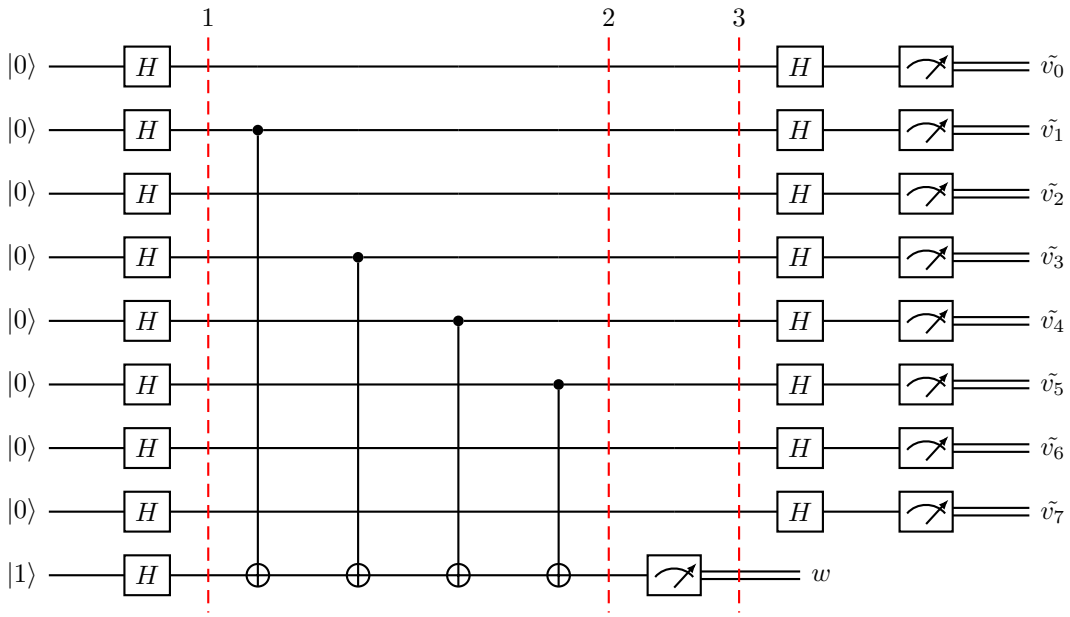


Figure 7: Example Circuit for Bernstein-Vazirani Algorithm

so far and the x_i symbols are placeholders for unknown values. We trace the execution symbolically:

$$\begin{aligned} |x_0x_1x_2x_3x_4x_5x_6x_7F()\rangle &\leftarrow |x_0x_1x_2x_3x_4x_5x_6x_7F(x_5)\rangle \\ &\leftarrow |x_0x_1x_2x_3x_4x_5x_6x_7F(x_4,x_5)\rangle \\ &\leftarrow |x_0x_1x_2x_3x_4x_5x_6x_7F(x_3,x_4,x_5)\rangle \\ &\leftarrow |x_0x_1x_2x_3x_4x_5x_6x_7F(x_1,x_3,x_4,x_5)\rangle \end{aligned}$$

For each operation $\textsc{cx}(x, v)$, we add x to the list of variables on which v depends. At the end of the execution, we conclude that x_1, x_3, x_4, and x_5 are the relevant qubits, from which we infer that the secret string must be 00111010.

4.2 E1

Consider the small circuit in Fig. 7. The scenario we are investigating is the following. The initial state of c_2, c_1, c_0 is unknown but both the initial state and final state of q_1, q_0 are known. The initial state is clearly 00 and let's assume for the remaining of this example that the final state is 01. The question is what can we infer about c_2, c_1, c_0? To answer the question, we will symbolically evaluate the circuit starting from the final state $c_0, c_1, c_2, 1, 0$ and going backwards towards the initial state as shown in Fig. 8. In step (1), we encounter a `cx` acting on q_1 and q_0 which are known. In step (2), we are not so lucky: we encounter a `ccx` gate with one unknown control wire but all hope is not lost. The action of `ccx` a b c is to update c to be $a \wedge b \oplus c$ where $\wedge$ is boolean conjunction (often omitted when clear from context) and $\oplus$ is the exclusive-or operation. In step (2), this means that the target wire q_1 should be updated to $1 \wedge c_0 \oplus 0$ which simplifies to c_0.

At the end of the retrodictive execution, we conclude that $q_0 = 1 \oplus c_0 \oplus c_1$ and $q_1 = c_0 \oplus c_2$ which needs to reconciled with the initial condition that $q_0 = q_1 = 0$. Solving these equations gives two possible solutions for $c_2 j, c_1, c_0$: either $c_2, c_1, c_0 = 010$ or $c_2, c_1, c_0 = 101$.

Another perspective on this analysis is the following. Assume c_2, c_1, c_0 started in an equal superposition and that q_1, q_0 were measured to be 01 after applying the circuit to the incoming superposition. The

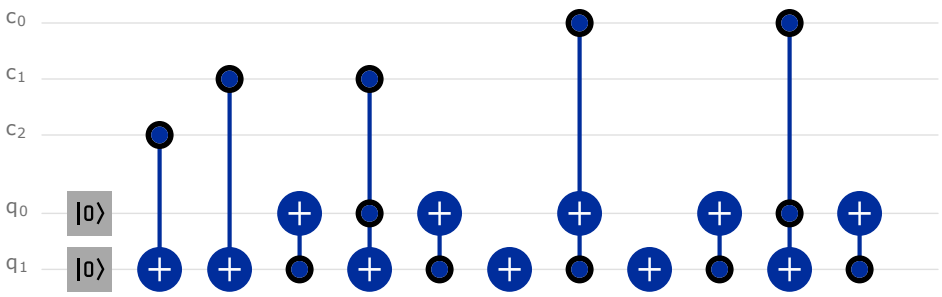


Figure 8: An Optimized Circuit for U_f where $f(x) = 4^x \mod 21$

measurement of q_1q_0 would essentially cause a *phase kickback* collapsing the equal superposition of all possible values of c_2, c_1, c_0 to just the two possible values that are consistent with the measurement.

4.3 E2

Fig. 9 shows a larger circuit. The top five wires are the interesting inputs while the bottom five wires serve as ancilla bits initialized to fixed values. The question we are interested in this case is the following: say we learn that at the end of the execution we have $b_2b_1b_0 = 001$, what possible input values for a_1a_0 and $b_2b_1b_0$ could have produced such a result? Using the same process as above, we calculate $b_0 = 1 \oplus a_0 \oplus a_1$, $b_1 = a_1 \oplus a_0a_1$, and $b_2 = 0$.

4.4 Perspective

Quantum algorithms typically operate on a *black box* holding a classical function whose properties need to be computed. The general structure of these algorithms is to (i) create a superposition of values to be passed as inputs to the black box, (ii) apply the operation inside the black box, and (iii) post-process the output of the black box. We observe that, in quite a few cases, steps (i) and (iii) are actually unnecessary and that the entire "quantum" algorithm can be executed by forward or backward, full or partial, efficient classical *symbolic execution* of the black box.

typical use: superposition, Uf, measure second register; we only care about which x has f(x) = r

By default all functions are reversible.

To make them irreversible you fix h and delete g. If you delete too much the function becomes very expensive to reverse. So one way functions emerge

simplify function has polynomial realization and we want statistics about the kernel (not necessarily compute it exactly)

collect assumptions:

important that no matter what measurement we do on w, properly we want is the same

since we say that algos related to pre-images lets do naive thing and eval backwards

assumptions we have a rev circuit efficient forward two inputs: first is full superposition; second whatever first output same as first input; but that is only at point 2; at point 3 explain kick back; misleading to think it is the same after 3 second output is result of function; measure; have element of range; go back with that elem if we knew first output as well as w then eval backwards same complexity but we only know w and we don't know first output; because we are starting at 3 not 2

we have no use for H block; it was only there for the forward exec to express our complete ignorance o the future; prepared with every x but if we have knowledge about future (w measured) we go back to find the values of x in the present that would be consistent with w so general circuit reduces to :

$$c_0\ c_1\ c_2\ (q_0 = 1)\ (q_1 = 0) \tag{0}$$

$(\texttt{cx}\ q_1\ q_0)$

$$c_0\ c_1\ c_2\ (q_0 = 1)\ (q_1 = 0) \tag{1}$$

$(\texttt{ccx}\ c_0\ q_0\ q_1)$

$$c_0\ c_1\ c_2\ (q_0 = 1)\ (q_1 = c_0) \tag{2}$$

$(\texttt{cx}\ q_1\ q_0)$

$$c_0\ c_1\ c_2\ (q_0 = 1 \oplus c_0)\ (q_1 = c_0) \tag{3}$$

$(\texttt{x}\ q_1)$

$$c_0\ c_1\ c_2\ (q_0 = 1 \oplus c_0)\ (q_1 = 1 \oplus c_0) \tag{4}$$

$(\texttt{ccx}\ c_0\ q_1\ q_0)$

$$c_0\ c_1\ c_2\ (q_0 = 1 \oplus c_0)\ (q_1 = 1 \oplus c_0) \tag{5}$$

$(\texttt{x}\ q_1)$

$$c_0\ c_1\ c_2\ (q_0 = 1 \oplus c_0)\ (q_1 = c_0) \tag{6}$$

$(\texttt{cx}\ q_1\ q_0)$

$$c_0\ c_1\ c_2\ (q_0 = 1)\ (q_1 = c_0) \tag{7}$$

$(\texttt{ccx}\ c_1\ q_0\ q_1)$

$$c_0\ c_1\ c_2\ (q_0 = 1)\ (q_1 = c_0 \oplus c_1) \tag{8}$$

$(\texttt{cx}\ q_1\ q_0)$

$$c_0\ c_1\ c_2\ (q_0 = 1 \oplus c_0 \oplus c_1)\ (q_1 = c_0 \oplus c_1) \tag{9}$$

$(\texttt{cx}\ c_1\ q_1)$

$$c_0\ c_1\ c_2\ (q_0 = 1 \oplus c_0 \oplus c_1)\ (q_1 = c_0) \tag{10}$$

$(\texttt{cx}\ c_2\ q_1)$

$$c_0\ c_1\ c_2\ (q_0 = 1 \oplus c_0 \oplus c_1)\ (q_1 = c_0 \oplus c_2) \tag{11}$$

Figure 9: Retrodictive execution of the circuit in Fig. 7

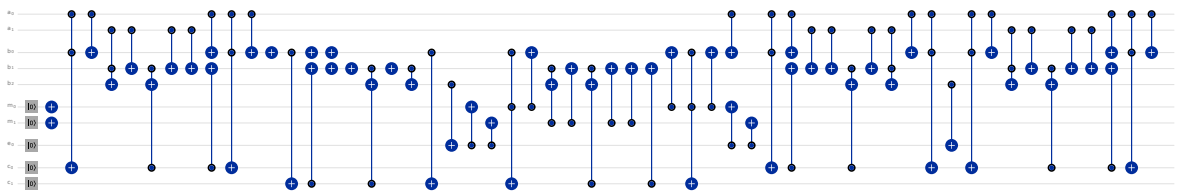


Figure 10: A Circuit for 2-bit Carry Adder

...

fix pics to have amplitudes with y (most general)

To what extent are the quantum algorithms above taking advantage of non-classical features. We posit that pre-image computation can be, at least for some of the some of the algorithms, be performed classically. The main insight needed for that is to perform the execution *symbolically*. We illustrate the idea with two examples.

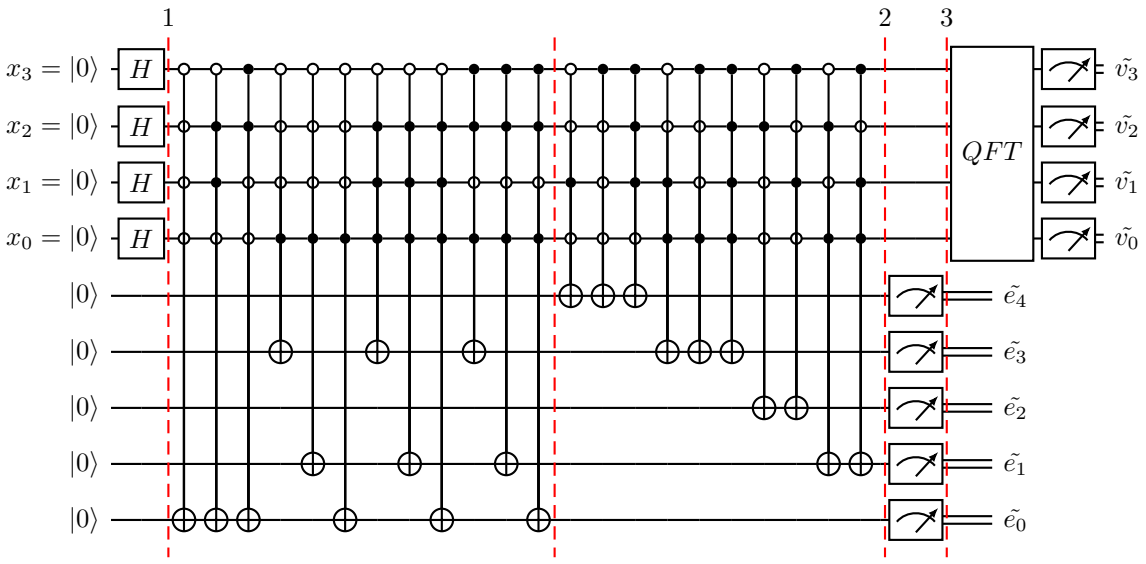


Figure 11: Finding the period of $11^x \mod 21$

5 Two Small Factoring Problems

5.1 Factoring 15

$$\begin{array}{rcl}
(1/\sqrt{6})\ |++{+}000\rangle & = & (1/\sqrt{12})\ (|++0000\rangle + |++1000\rangle) \\
& \rightarrow & (1/\sqrt{12})\ (|++1000\rangle + |++0000\rangle) \\
& \rightarrow & (1/\sqrt{12})\ (|++1001\rangle + |++0000\rangle) \\
& \rightarrow & (1/\sqrt{12})\ (|++0001\rangle + |++1000\rangle) \\
& \rightarrow & (1/\sqrt{12})\ (|++0001\rangle + |++1100\rangle)
\end{array}$$

Say we measure 001 in the second register. The state of the first register collapses to $(1/\sqrt{3})\ |++0\rangle$ which is given to the QFT block. The QFT result is $(1/\sqrt{2})\ (|\tilde{0}\tilde{0}0\rangle + |\tilde{1}\tilde{0}0\rangle)$. If measure 0 we repeat the experiment. If we measure 4 we infer that the period is $8/4 = 2$ and hence that the factors are 3 and 5.

Now do retrodictive execution starting with $|x_2x_1x_0001\rangle$:

$$\begin{array}{rcl}
|x_2x_1x_0001\rangle & \rightarrow & |x_2x_1x_0x_001\rangle \\
& \rightarrow & |x_2x_1\overline{x_0}x_001\rangle \\
& \rightarrow & |x_2x_1\overline{x_0}x_00x_0\rangle \\
& \rightarrow & |x_2x_1x_0x_00x_0\rangle
\end{array}$$

Initial condition says $x_0 = 0$ and hence the pre-image is ??0 which matches $000, 010, 100, 110$, i.e., the period is 2.

5.2 Factoring 21

$$|0000\rangle|00000\rangle + |0001\rangle|00000\rangle + |0010\rangle|00000\rangle + |0011\rangle|00000\rangle + |0100\rangle|00000\rangle + |0101\rangle|00000\rangle + |0110\rangle|00000\rangle + |0111\rangle|00000\rangle + |1000\rangle|00000\rangle + |1001\rangle|00000\rangle + |1010\rangle|00000\rangle + |1011\rangle|00000\rangle + |1100\rangle|00000\rangle + |1101\rangle|00000\rangle + |1110\rangle|00000\rangle + |1111\rangle|00000\rangle$$

$$\rightarrow |0000\rangle|00001\rangle + |0001\rangle|01011\rangle + |0010\rangle|00000\rangle + |0011\rangle|00000\rangle + |0100\rangle|00000\rangle + |0101\rangle|00000\rangle + |0110\rangle|00001\rangle + |0111\rangle|01011\rangle + |1000\rangle|00000\rangle + |1001\rangle|00000\rangle + |1010\rangle|00000\rangle + |1011\rangle|00000\rangle + |1100\rangle|00001\rangle + |1101\rangle|01011\rangle + |1110\rangle|00000\rangle + |1111\rangle|00000\rangle$$

$$\rightarrow |0000\rangle|00001\rangle + |0001\rangle|01011\rangle + |0010\rangle|10000\rangle + |0011\rangle|01000\rangle + |0100\rangle|00100\rangle + |0101\rangle|00010\rangle + |0110\rangle|00001\rangle + |0111\rangle|01011\rangle + |1000\rangle|10000\rangle + |1001\rangle|01000\rangle + |1010\rangle|00010\rangle + |1011\rangle|00010\rangle + |1100\rangle|00001\rangle + |1101\rangle|01011\rangle + |1110\rangle|10000\rangle + |1111\rangle|01000\rangle$$

$$\rightarrow (|0000\rangle + |0110\rangle + |1100\rangle)|00001\rangle + (|0101\rangle + |1011\rangle)|00010\rangle + (|0100\rangle + |1010\rangle)|00100\rangle + (|0011\rangle + |1001\rangle + |1111\rangle)|01000\rangle + (|0001\rangle + |0111\rangle + |1101\rangle)|01011\rangle + (|0010\rangle + |1000\rangle + |1110\rangle)|10000\rangle$$

Say we measure 01011 in second register, the state collapses to $|0001\rangle + |0111\rangle + |1101\rangle$. QFT probabilities are:

$$\begin{array}{rcl} |\tilde{0}\rangle & : & 19\% \\ |\tilde{8}\rangle & : & 19\% \\ |\tilde{3}\rangle & : & 12\% \\ |\tilde{5}\rangle & : & 12\% \\ |\tilde{11}\rangle & : & 12\% \\ |\tilde{13}\rangle & : & 12\% \\ |\tilde{2}\rangle & : & 2\% \\ |\tilde{4}\rangle & : & 2\% \\ |\tilde{6}\rangle & : & 2\% \\ |\tilde{10}\rangle & : & 2\% \\ |\tilde{12}\rangle & : & 2\% \\ |\tilde{14}\rangle & : & 2\% \end{array}$$

Continued fraction: measure 8, should be close to m16/r, gives us r=2 bad
measure 3; should be close to m16/r; gives us r = 5; odd bad measure 5; bad measure 11
gcd 10 21

```
m16/r ~ 11

11/16 ~ m/r

11/16 = 1/(1+5/11) = 1/(1+(1/2+1/5))
```

6 Retrodictive

6.1 Retrodictive Classical Computation

Were we lucky in these two examples or is there something interesting happening; we can use ideas from physics that are not all quantum to try to improve classical computation

We need to explain ideas about time-reversal, prediction and retrodiction in physics. The laws of computation and the laws of physics are intimately related. When does knowing something about the future help us unveil the structure or symmetries of the past? It is like a detective story, but one with ramifications in complexity and/or efficiency. Problems involving questions where answers demand a Many(past)-to-one(future) map are at the root of our proposal.... Difference between exploiting or not entanglement in the unitary evolution.

As we demonstrate, the family of quantum algorithms initiated by Deutsch's algorithm and culminating with Shor's algorithm (i) solves variants of the pre-image problem efficiently, and, in that context, (ii) answering queries about pre-images is closely related to *retrodictive quantum theory* [2], retrocausality [1], and the time-symmetry of physical laws [5].

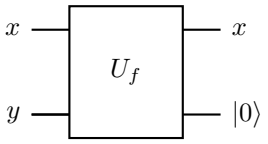
- Retrodictive execution more efficient in some cases. What cases?
- Here are three examples: Deutsch-Jozsa, Simon, Shor when period is close to a power of 2
- Symbolic (retrodictive) evaluation as a broader perspective to classical computation
- Symbolic execution allows you to express/discover interference via shared variables
- When interference pattern is simple symbolic execution reveals solutions faster (and completely classically)
- Symbolic execution as a "classical waves" computing paradigm

to represent unequal superpositions do multiple runs with vars the first has x1 x2 etc the second has y1 2y2 etc or y2/2 etc, or with various patterns of negative weights.... And then the punchline would be to interpret the negative backwards. So instead of all forward or all retro we have some values going forward and then backwards

Start with the story about function many to one etc why superpositions because we don't know which values so we try all easy to represent by unknown vars so we can represent superpositions as vars and equations between them but at the end we want stats about superpositions slow way is to generate all equations and solve faster way is generate many sets of equations with different weights and sum to get your stats

6.2 Deutsch

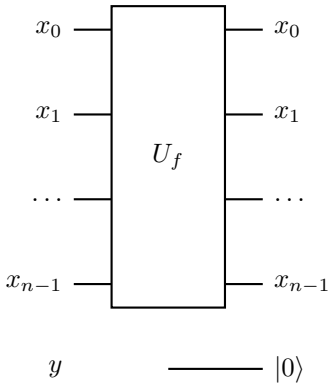
The problem is to determine if a function $[\mathbf{2}] \to [\mathbf{2}]$ is constant or balanced. The only relevant part of the circuit is:



We fix the ancillary output to a possible boundary condition, say $|0\rangle$, and perform a retrodictive execution of the circuit. This execution produces a formula for y that depends on the function f in the black box. When the function f is a constant function, the formula is the corresponding constant 0 or 1. When the function is balanced the resulting formula is x (when the function is the identity) or $1+x$ (when the function is boolean negation).

6.3 Deutsch-Jozsa

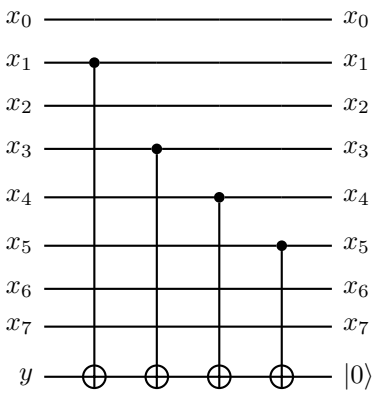
The problem is a generalization of the previous one: the question is to determine if a function $\mathbb{B}^n \to \mathbb{B}$ is constant or balanced. The circuit is identical to above except that x is now a collection of qubits:



Again, we fix the ancillary output to a possible boundary condition, say $|0\rangle$, and perform a retrodictive execution of the circuit. This execution produces a formula for y that depends on the function f in the black box. When the function f is a constant function, the formula is the corresponding constant 0 or 1. When the function is balanced the resulting formula involves at least one variable x_i.

6.4 Bernstein-Vazirani

The circuit below gives the definition of the oracle U_f for an instance of the problem where $n = 8$ and the hidden number s is 00111010:

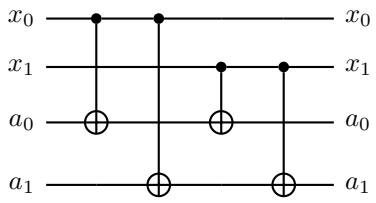


We can ignore all the parts of the circuits and just focus on symbolically running the circuit in a retrodictive fashion to compute the pre-image of 0. The first gate is cx x5 0 which the last wire to x5; the next is cx x4 x5 which sets the last wire to x4 xor x5 and so on. reveals that $y = x_1 \oplus x_3 \oplus x_4 \oplus x_5$ which are exactly the bits that are equal to 1 in the hidden string. the query can be answered directly and we didn't need anything exponential in this case

6.5 Simon

We are given a 2-1 function $f : \mathbb{B}^n \to \mathbb{B}^n$ where there exists an a such $f(x) = f(x \oplus a)$ for all x; the goal is to determine a.

The circuit below demonstrates the situation when $n = 2$ and $a = 3$.



The circuit implements the black box $U_f(x, a) = (x, f(x) \oplus a)$. We first pick a random x, say $x = 3$, fix the initial condition $a = 0$ and run the circuit forward. This execution produces, in the second register, the value of $f(x) = 0$. We now run a symbolic retrodictive execution with $a = 0$ at the output site. That execution produces information on all values of a that are consistent with the observed result. In this case, we get: $a_0 = x_0 + x_1$ and $a_1 = x_0 + x_1$. In other words, when $x_0 = x_1$, we have $a = 0$, and when $x_0 \neq x_1$, we have $a = 3$ which is indeed the desired hidden value.

7 Partial Symbolic Evaluation with Algebraic Normal Form (ANF)

We should use two prototypical examples to illustrate main ideas before going to the complex ones. The examples I have in mind are: Deutsch-Josza and Simon (precursor of Shor's). There are prior works on dequantization of the first problem and should make contact with their resolution. Perhaps we can show that they are as efficient classically? That would justify retrodiction alone. The more complex (and important) case of factorization should be the natural follow up.

The idea of symbolic execution is not tied to forward or backward execution. We should introduce it in a way that is independent of the direction of execution. What the idea depends on however is that the wave function, at least in the cases we are considering, can be represented as equations over booleans.

Wave Functions as Equations over Booleans

in the typical scenario for using quantum oracles, we can represent wave function as equations over booleans; equations represent the wave function but the solution is unobservable just like the components of the superposition in the wave function are not observable; just like we don't directly get access to the components of the wave function; we don't directly get access to the solution of the equations; need to "observe" the equations

we can go backwards with an equation (representing a wave function sigma x where f(x) = r and go back towards the present to calculate the wave function (represented as equations again)

Musing: how to explain complementarity when wave function is represented as an equation? Kochen specker;

or contextuality

observer 1 measures wires a,b; obs2 measures wires b,c; not commuting; each obs gives partial solution to equations; but partial solutions cannot lead to a global solution

KS suggests that equations do not have unique solutions; only materialize when you measure;

can associate a probability with each variable in a equation: look at all solutions and see the contribution of each variable to these solutions.

8 Complexity Analysis

one pass over circuit BUT complexity of normalizing to ANF not trivial; be careful

9 Conclusion

Provide a general introduction to the topic and a brief non-technical summary of your main results and their implication.

200 words ??
main text 2000-2500 words 3-4 figures 30-50 references
Methods section 3000 words more references ok
Author contributions
Code available
https://quantumalgorithmzoo.org
every quantum circuit can be written using Toffoli and Hadamard retro just go through Toffoli; ignore Had; but of course we are using symbolic eval
can H be moved past Toffoli?
universe uses lazy evaluation?
algebra of Toffoli and Hadamard ZX calcululs
fourier transform classical efficient in some cases
Ewin Tang papers
kochen specker ??

References

[1] Yakir Aharonov and Lev Vaidman. "The Two-State Vector Formalism: An Updated Review". In: *Time in Quantum Mechanics*. Ed. by J.G. Muga, R. Sala Mayato, and Í.L. Egusquiza. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 399–447.

[2] Stephen M. Barnett, John Jeffers, and David T. Pegg. "Quantum Retrodiction: Foundations and Controversies". In: *Symmetry* 13.4 (2021).

[3] Yoshihiko Futamura. "Partial computation of programs". In: *RIMS Symposia on Software Science and Engineering*. Ed. by Eiichi Goto, Koichi Furukawa, Reiji Nakajima, Ikuo Nakata, and Akinori Yonezawa. Berlin, Heidelberg: Springer Berlin Heidelberg, 1983, pp. 1–35.

[4] Peter Henderson and James H. Morris. "A Lazy Evaluator". In: *Proceedings of the 3rd ACM SIGACT-SIGPLAN Symposium on Principles on Programming Languages*. POPL '76. Atlanta, Georgia: Association for Computing Machinery, 1976, pp. 95–103.

[5] Satosi Watanabe. "Symmetry of Physical Laws. Part III. Prediction and Retrodiction". In: *Rev. Mod. Phys.* 27 (2 Apr. 1955), pp. 179–186.