

De-Quantizing Quantum Algorithms by Retrodictive Execution

Jacques Carette
McMaster University

Gerardo Ortiz*
Indiana University

Amr Sabry
Indiana University

February 14, 2022

Abstract

The quantum circuit model consists of two classes of gates: (i) quantum counterparts to classical reversible gates (e.g., Toffoli gates), and (ii) genuine quantum gates with no classical counterpart (e.g., Hadamard and phase gates). We make the remarkable observation, that, for a number of well-established quantum algorithms, judicious reasoning about the classical components, ignoring all the quantum gates, is sufficient. Put differently, in those cases, the quantum gates serve no fundamental purpose and are actually distracting from an underlying efficient classical algorithm. The result relies on the ability to symbolically execute circuits, especially in a retrodictive fashion, i.e., by making partial observations at the output site and proceeding backwards to infer the implied initial conditions.

1 Main

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

Retrodictive quantum theory [3], retrocausality [1], and the time-symmetry of physical laws [11] 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* [6] and *symbolic partial evaluation* [5], retrodictive reasoning can be used as a computational resource to de-quantize some quantum algorithms, i.e., to provide efficient classical algorithms inspired by their quantum counterparts.

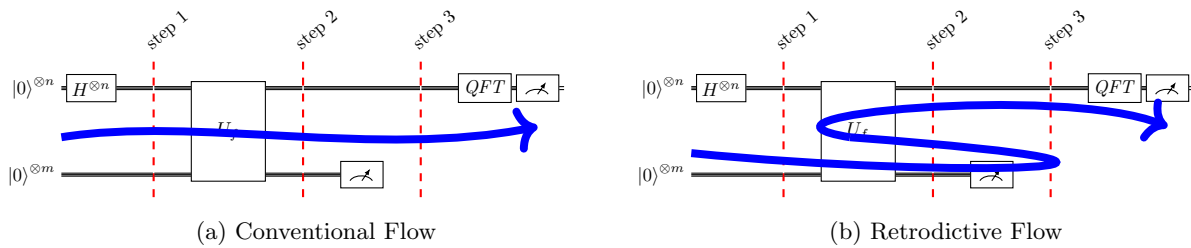


Figure 1: Template quantum circuit

Many quantum algorithms can be expressed using circuits consisting of three stages: preparation, unitary evolution, and measurement in the Hadamard / Fourier basis as shown in Fig. 1(a). The unitary evolution block is typically a quantum oracle U_f that encapsulates a classical function f to be analyzed. 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 forward direction to produce the outputs. Retrodictive reasoning suggests more creative ways to execute the U_f block as shown in Fig. 1(b). In this model, a forward execution is performed to determine a possible measurement result for the bottom

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

Figure 3: Equations generated by retrodictive execution of $a^x \bmod 15$ starting from observed result 1 and unknown $x_8 x_7 x_6 x_5 x_4 x_3 x_2 x_1 x_0$. The solution for the unknown variables is given in the last column.

register; using this information, a retrodictive execution is performed to determine the initial states of the first register that are consistent with this measurement. These states are then propagated forward to the measurement process.

In order to assess whether this idea works for a broad 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. As we demonstrate below, it turns that retrodictive symbolic evaluation provides additional *classical* computational resources that are powerful enough to solve instances of Deutsch-Jozsa, Bernstein-Vazirani, and Simon problems, as well as some instances of Grover’s and Shor’s algorithms. In all the problems below, let $[n]$ denote the finite set $\{0, 1, \dots, (n-1)\}$. The parameter n determines the problem size and the goal is to solve the problem using resources that do not grow exponentially in n .

Shor 15. The circuit in Fig. 2 uses a hand-optimized implementation of the modular exponentiation $4^x \bmod 15$ to factor 15 using Shor’s algorithm. In a conventional forward execution, the state at step (3) is:

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

At this point, the bottom 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 $|0\rangle$ for the top register, 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 $|x_2 x_1 x_0\rangle |001\rangle$ at step (2) and compute backwards. The first

CX-gate changes the state to $|x_2 x_1 x_0\rangle |x_0 01\rangle$ and the second CX-gate produces $|x_2 x_1 x_0\rangle |x_0 0 x_0\rangle$. At that point, we reconcile the retrodictive result of the second register $|x_0 0 x_0\rangle$ with the initial condition $|000\rangle$ to conclude that $x_0 = 0$. In other words, in order to observe $e_2 e_1 e_0 = 001$, the first register must be initialized to a superposition 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 needs to be in a superposition of the states $|000\rangle, |010\rangle, |100\rangle$ or $|110\rangle$ and we have just inferred using purely classical but retrodictive reasoning that the period is 2. Significantly, this approach is robust and does not require small hand-optimized circuits. Indeed, following the methods for producing quantum circuits for arithmetic operations from first principles using adders and multipliers [10], our implementation for $a^x \bmod 15$ has 56538 generalized Toffoli gates over 9 qubits, and yet the equations resulting from the retrodictive execution in Fig. 3 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.

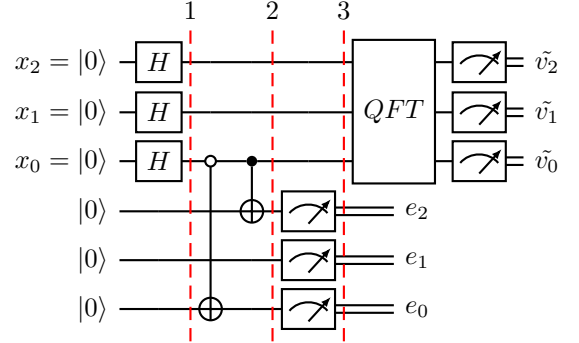


Figure 2: Finding the period of $4^x \bmod 15$

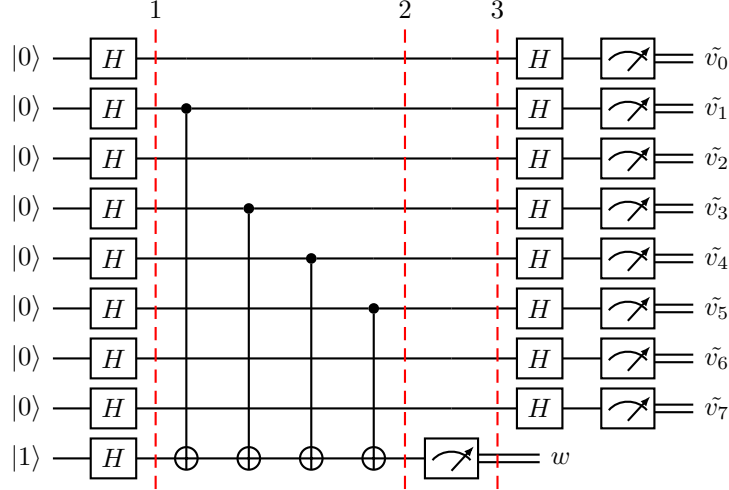


Figure 4: Circuit for Bernstein-Vazirani Algorithm ($n = 8$, $s = 92$, least significant bit is the top wire)

Deutsch. The problem is to determine if a given function $[2] \rightarrow [2]$ is constant or balanced. It is assumed that the function is embedded in a quantum circuit U_f , typically composed of X and CX gate, and the goal is to use U_f just once. The textbook quantum algorithm prepares a quantum superposition that propagates through the quantum oracle U_f in the forward direction and then performs a measurement that deterministically solves the problem. Instead, we fix the ancilla output to a possible boundary condition, say $|0\rangle$, provide a symbolic state $|x\rangle$ for the top register, and perform a retrodictive execution of the quantum oracle. The execution starts from the output side with the state $|x\rangle|0\rangle$ and terminates on the input side with a state $|x\rangle|y\rangle$ where y is a symbolic expression that captures the necessary initial conditions to produce the partial observation $|0\rangle$ on the ancilla register. Running the experiment, we get one of the following four symbolic expressions 0, 1, x , or $1 \oplus x$ depending on the function f . In the first two cases, the observation of the ancilla is independent of x , i.e. the function is constant. In the last two cases, the ancilla depends on x (or its negation), and the function must be balanced.

Deutsch-Jozsa. The problem is a generalization of the previous one: we are given a function $[n] \rightarrow [2]$ that is promised to be constant or balanced and we need to decide distinguish the two cases. Again, we fix the ancillary output to a possible boundary condition, say $|0\rangle$, and perform a retrodictive execution of the circuit to calculate a symbolic expression. Running the experiment for the two constant functions, the result is 0 or 1 indicating no dependency of the ancilla on the input. For three examples of balanced functions with $n = 6$, the resulting expression was x_0 in one case, $x_0 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5$ in another, and $x_0x_1x_2 \oplus x_0x_1x_2x_3x_4 \oplus x_0x_1x_2x_3x_5 \oplus x_0x_1x_2x_4x_5 \oplus x_0x_1x_2x_4x_5 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3x_5 \oplus x_0x_1x_4 \oplus x_0x_1x_4x_5 \oplus x_0x_2 \oplus x_0x_2x_3x_5 \oplus x_0x_2x_4x_5 \oplus x_0x_3 \oplus x_0x_3x_4x_5 \oplus x_0x_3x_5 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_4x_5 \oplus x_1x_3x_4x_5 \oplus x_1x_3x_5 \oplus x_1x_5 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_5 \oplus x_2x_4 \oplus x_3x_4x_5 \oplus x_3x_5$ in the last. In the first case, the function is balanced because its output depends on just one variable (which is 0 half the time); in the second case the output of the function is the exclusive-or of all the input variables which is an easy instance of a balanced function. The last case is a cryptographically strong balanced function whose output pattern is, by design, difficult to discern [4]. Since we are promised the function is either constant or balanced, then any output that depends on at least one symbolic variable is incompatible with a constant function; the details of the dependency are not relevant.

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

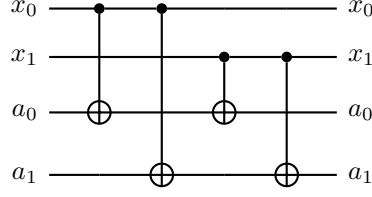


Figure 5: Example of Quantum Oracle for Simon's Algorithm

91 as $f(x) = \sum_{i=0}^{n-1} s_i x_i \bmod 2$. The goal is to determine the secret number s . The circuit in Fig. 4 solves
 92 the problem for $n = 8$ and a hidden number 92 (= 00111010 in binary notation with the rightmost bit at
 93 index 0). The gates between slice (1) and slice (2) collect the sum of the x_i at positions that match the
 94 occurrences of 1 in the secret string. The retrodictive execution proceeds from slice (2) backwards with the
 95 state $|x_0 x_1 x_2 x_3 x_4 x_5 x_6 x_7 0\rangle$; upon termination the last qubit has the symbolic value $x_1 \oplus x_3 \oplus x_4 \oplus x_5$. The
 96 indices $\{1, 3, 4, 5\}$ are exactly the positions in which the secret string has a 1.

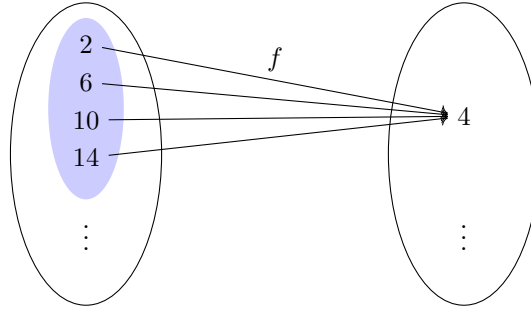
97 **Simon.** We are given a 2-1 function $f : [2^n] \rightarrow [2^n]$ with the property that there exists an a such $f(x) =$
 98 $f(x \oplus a)$ for all x ; the goal is to determine a . The circuit in Fig. 5 demonstrates the situation when $n = 2$
 99 and $a = 3$. In order to perform retrodictive execution, we need a possible final value for $a_1 a_0$ with which
 100 to initiate the backwards execution. For that we simply *classically* execute the circuit once in the forward
 101 direction with a random choice of $x_1 x_0$ (say $x_1 x_0 = 11$) and an initial condition $a_1 a_0 = 00$. This execution
 102 results in $a_1 a_0 = 00$ giving us a possible future observation. The goal now is to find the other possible
 103 value for $x_1 x_0$ that produces this observation and for that we simply run backwars with the symbolic state
 104 $|x_0 x_1 00\rangle$. The result is the equation $x_0 \oplus x_1 = 0$ whose only two solutions are $x_1 x_0 = 00$ or $x_1 x_0 = 11$.

Grover
Shor again (21 huge)

Pre-images and NP-Complete Problems. we have some success stories

but Shor 21 huge
let's understand pre-image NP etc.
need stats only
PEX , PEY ...

Given finite sets A and B , a function $f : A \rightarrow B$ and an element $y \in B$, we define $\{ \cdot \stackrel{f}{\leftarrow} y \}$, the pre-image of y under f , as the set $\{x \in A \mid f(x) = y\}$. For example, let $A = B = \{0, 1, \dots, 15\}$ and let $f(x) = 7^x \bmod 15$, then the collection of values that f maps to 4, $\{ \cdot \stackrel{f}{\leftarrow} 4 \}$, 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 [9], predicting environmental conditions that allow certain reactions to take place in computational biology [2, 7], and finding the pre-image of feature vectors in the space induced by a kernel in neural networks [8].

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.

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

Deutsch. The conventional statement of the problem is to determine if a function $[2] \rightarrow [2]$ 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.

DJ. The problem is a generalization of the previous one: the question is to determine if a function $[2^n] \rightarrow [2]$ 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.

BV. 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 $f : [2^n] \rightarrow [2^n]$ 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 $f(x) = a^x \bmod 2^n$ 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 of two inputs; two outputs system; ancilla; normal eval; control ancilla; system unknown; so throw in complete superposition and eval forward

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. ??.

Retrodictive QFT. only need number of vars !!!!

solve other problems with just knowing which vars are involved

Discussion. 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 calculus

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] Tatsuya Akutsu, Morihiro Hayashida, Shu-Qin Zhang, Wai-Ki Ching, and Michael K Ng. "Analyses and algorithms for predecessor and control problems for Boolean networks of bounded indegree". In: *Information and Media Technologies* 4.2 (2009), pp. 338–349.
- [3] Stephen M. Barnett, John Jeffers, and David T. Pegg. "Quantum Retrodiction: Foundations and Controversies". In: *Symmetry* 13.4 (2021).
- [4] Linda Burnett, William Millan, Edward Dawson, and Andrew Clark. "Simpler Methods for Generating Better Boolean Functions with Good Cryptographic Properties". In: *Australasian Journal of Combinatorics* 29 (2004), pp. 231–247.

- [5] 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.
- [6] 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.
- [7] Johannes Georg Klotz, Martin Bossert, and Steffen Schober. “Computing preimages of Boolean networks”. In: *BMC Bioinformatics* 14.10 (Aug. 2013), S4.
- [8] J.T.-Y. Kwok and I.W.-H. Tsang. “The pre-image problem in kernel methods”. In: *IEEE Transactions on Neural Networks* 15.6 (2004), pp. 1517–1525.
- [9] Phillip Rogaway and Thomas Shrimpton. “Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance”. In: *Fast Software Encryption*. Ed. by Bimal Roy and Willi Meier. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 371–388.
- [10] Vlatko Vedral, Adriano Barenco, and Artur Ekert. “Quantum networks for elementary arithmetic operations”. In: *Phys. Rev. A* 54 (1 July 1996), pp. 147–153.
- [11] Satoshi Watanabe. “Symmetry of Physical Laws. Part III. Prediction and Retrodiction”. In: *Rev. Mod. Phys.* 27 (2 Apr. 1955), pp. 179–186.

2 Methods

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 site 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.

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

```
238 power :: Int -> Int -> Int
239 power a n
240   | n == 0      = 1
241   | n == 1      = a
242   | even n      = let r = power a (n `div` 2) in r * r
243   | otherwise   = a * power a (n-1)
```

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

```
245     power 3 5
246 = 3 * power 3 4
247 = 3 * (let r1 = power 3 2 in r1 * r1)
248 = 3 * (let r1 = (let r2 = power 3 1 in r2 * r2) in r1 * r1)
249 = 3 * (let r1 = (let r2 = 3 in r2 * r2) in r1 * r1)
250 = 3 * (let r1 = 9 in r1 * r1)
251 = 243
```

252 Partial evaluation is used when we only have partial information about the inputs. Say we only know
 253 $n = 5$. A partial evaluator then attempts to evaluate `power` with symbolic input `a` and actual input `n=5`.
 254 This evaluation proceeds as follows:

```
255     power a 5
256 = a * power a 4
257 = a * (let r1 = power a 2 in r1 * r1)
258 = a * (let r1 = (let r2 = power a 1 in r2 * r2) in r1 * r1)
259 = a * (let r1 = (let r2 = a in r2 * r2) in r1 * r1)
260 = a * (let r1 = a * a in r1 * r1)
261 = let r1 = a * a in a * r1 * r1
```

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

264 The evolution of a quantum system is typically understood as proceeding forwards in time — from the
 265 present to the future. As shown in Fig. 1(a),

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

271 **Data Availability.** available

272 **Discussion.** Possibility that collapse of wave function is information flow back from measured future to
 273 present unknown initial conditions and then back to rest of wave that was not measured
 274 transactional interpretation?

275 Luckily, the problems of concern to us are quite special: (i) the functions are not arbitrary but have
 276 additional structure that can be exploited, and (ii) we never need access to all the elements in the pre-image;
 277 we just need to answer aggregate queries about the pre-images. Quantum algorithms somehow exploit these
 278 properties along with some physical principles to solve these problems efficiently. To understand the precise
 279 way in which this is happening, we start with the template of the quantum circuit used for solving all the
 280 problems above in Fig. 1.

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.

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, U_f , 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 of 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 :

...

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.

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 [4].

- 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 $x_1 x_2$ etc the second has $y_1 2y_2$ etc or $y_2/2$ 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

Partial Symbolic Evaluation with Algebraic Normal Form (ANF). The resulting expressions are in algebraic normal form [3] where $+$ denotes exclusive-or.

We should use two prototypical examples to illustrate main ideas before going to the complex ones. The examples I have in mind are: Deutsch-Jozsa and Simon (precursor of Shor's). There are prior works on de-quantization 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 σ 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.

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

Supplementary Information. Equations generated by retrodictive execution of $4^x \bmod 21$ 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.

$$\begin{aligned}
& 1 \oplus x_0 \oplus x_0 x_1 x_2 \oplus x_0 x_1 x_2 x_3 x_4 \oplus x_0 x_1 x_2 x_3 x_4 x_5 x_6 \oplus x_0 x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8 \oplus x_0 x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_9 \oplus x_0 x_1 x_2 x_3 x_4 x_5 x_6 x_8 \oplus \\
& x_0 x_1 x_2 x_3 x_4 x_5 x_6 x_8 x_9 \oplus x_0 x_1 x_2 x_3 x_4 x_5 x_7 \oplus x_0 x_1 x_2 x_3 x_4 x_5 x_7 x_8 x_9 \oplus x_0 x_1 x_2 x_3 x_4 x_5 x_7 x_9 \oplus x_0 x_1 x_2 x_3 x_4 x_5 x_8 \oplus \\
& x_0 x_1 x_2 x_3 x_4 x_5 x_9 \oplus x_0 x_1 x_2 x_3 x_4 x_6 \oplus x_0 x_1 x_2 x_3 x_4 x_6 x_7 \oplus x_0 x_1 x_2 x_3 x_4 x_6 x_7 x_8 \oplus x_0 x_1 x_2 x_3 x_4 x_6 x_7 x_8 x_9 \oplus x_0 x_1 x_2 x_3 x_4 x_6 x_8 x_9 \oplus \\
& x_0 x_1 x_2 x_3 x_4 x_6 x_9 \oplus x_0 x_1 x_2 x_3 x_4 x_7 x_8 \oplus x_0 x_1 x_2 x_3 x_4 x_7 x_9 \oplus x_0 x_1 x_2 x_3 x_4 x_8 \oplus x_0 x_1 x_2 x_3 x_4 x_8 x_9 \oplus x_0 x_1 x_2 x_3 x_5 \oplus \\
& x_0 x_1 x_2 x_3 x_5 x_6 x_7 \oplus x_0 x_1 x_2 x_3 x_5 x_6 x_7 x_8 x_9 \oplus x_0 x_1 x_2 x_3 x_5 x_6 x_7 x_9 \oplus x_0 x_1 x_2 x_3 x_5 x_6 x_8 \oplus x_0 x_1 x_2 x_3 x_5 x_6 x_9 \oplus x_0 x_1 x_2 x_3 x_5 x_7 \oplus \\
& x_0 x_1 x_2 x_3 x_5 x_7 x_8 \oplus x_0 x_1 x_2 x_3 x_5 x_7 x_8 x_9 \oplus x_0 x_1 x_2 x_3 x_5 x_8 x_9 \oplus x_0 x_1 x_2 x_3 x_5 x_9 \oplus x_0 x_1 x_2 x_3 x_6 \oplus x_0 x_1 x_2 x_3 x_6 x_7 x_8 \oplus \\
& x_0 x_1 x_2 x_3 x_6 x_7 x_9 \oplus x_0 x_1 x_2 x_3 x_6 x_8 \oplus x_0 x_1 x_2 x_3 x_6 x_8 x_9 \oplus x_0 x_1 x_2 x_3 x_7 \oplus x_0 x_1 x_2 x_3 x_7 x_8 x_9 \oplus x_0 x_1 x_2 x_3 x_7 x_9 \oplus \\
& x_0 x_1 x_2 x_3 x_8 \oplus x_0 x_1 x_2 x_3 x_9 \oplus x_0 x_1 x_2 x_4 \oplus x_0 x_1 x_2 x_4 x_5 \oplus x_0 x_1 x_2 x_4 x_5 x_6 \oplus x_0 x_1 x_2 x_4 x_5 x_6 x_7 \oplus x_0 x_1 x_2 x_4 x_5 x_6 x_7 x_8 \oplus \\
& x_0 x_1 x_2 x_4 x_5 x_6 x_7 x_8 x_9 \oplus x_0 x_1 x_2 x_4 x_5 x_6 x_8 x_9 \oplus x_0 x_1 x_2 x_4 x_5 x_6 x_9 \oplus x_0 x_1 x_2 x_4 x_5 x_7 x_8 \oplus x_0 x_1 x_2 x_4 x_5 x_7 x_9 \oplus x_0 x_1 x_2 x_4 x_5 x_8 \oplus \\
& x_0 x_1 x_2 x_4 x_5 x_8 x_9 \oplus x_0 x_1 x_2 x_4 x_6 x_7 \oplus x_0 x_1 x_2 x_4 x_6 x_7 x_8 x_9 \oplus x_0 x_1 x_2 x_4 x_6 x_7 x_9 \oplus x_0 x_1 x_2 x_4 x_6 x_8 \oplus x_0 x_1 x_2 x_4 x_6 x_9 \oplus \\
& x_0 x_1 x_2 x_4 x_7 \oplus x_0 x_1 x_2 x_4 x_7 x_8 \oplus x_0 x_1 x_2 x_4 x_7 x_8 x_9 \oplus x_0 x_1 x_2 x_4 x_8 x_9 \oplus x_0 x_1 x_2 x_4 x_9 \oplus x_0 x_1 x_2 x_5 x_6 \oplus x_0 x_1 x_2 x_5 x_6 x_7 x_8 \oplus \\
& x_0 x_1 x_2 x_5 x_6 x_7 x_9 \oplus x_0 x_1 x_2 x_5 x_6 x_8 \oplus x_0 x_1 x_2 x_5 x_6 x_8 x_9 \oplus x_0 x_1 x_2 x_5 x_7 \oplus x_0 x_1 x_2 x_5 x_7 x_8 x_9 \oplus x_0 x_1 x_2 x_5 x_7 x_9 \oplus \\
& x_0 x_1 x_2 x_5 x_8 \oplus x_0 x_1 x_2 x_5 x_9 \oplus x_0 x_1 x_2 x_6 \oplus x_0 x_1 x_2 x_6 x_7 \oplus x_0 x_1 x_2 x_6 x_7 x_8 \oplus x_0 x_1 x_2 x_6 x_7 x_8 x_9 \oplus x_0 x_1 x_2 x_6 x_8 x_9 \oplus \\
& x_0 x_1 x_2 x_6 x_9 \oplus x_0 x_1 x_2 x_7 x_8 \oplus x_0 x_1 x_2 x_7 x_9 \oplus x_0 x_1 x_2 x_8 \oplus x_0 x_1 x_2 x_8 x_9 \oplus x_0 x_1 x_3 \oplus x_0 x_1 x_3 x_4 x_5 \oplus x_0 x_1 x_3 x_4 x_5 x_6 x_7 \oplus \\
& x_0 x_1 x_3 x_4 x_5 x_6 x_7 x_8 x_9 \oplus x_0 x_1 x_3 x_4 x_5 x_6 x_7 x_9 \oplus x_0 x_1 x_3 x_4 x_5 x_6 x_8 \oplus x_0 x_1 x_3 x_4 x_5 x_6 x_9 \oplus x_0 x_1 x_3 x_4 x_5 x_7 \oplus x_0 x_1 x_3 x_4 x_5 x_7 x_8 \oplus \\
& x_0 x_1 x_3 x_4 x_5 x_7 x_8 x_9 \oplus x_0 x_1 x_3 x_4 x_5 x_8 x_9 \oplus x_0 x_1 x_3 x_4 x_5 x_9 \oplus x_0 x_1 x_3 x_4 x_6 \oplus x_0 x_1 x_3 x_4 x_6 x_7 x_8 \oplus x_0 x_1 x_3 x_4 x_6 x_7 x_9 \oplus \\
& x_0 x_1 x_3 x_4 x_6 x_8 \oplus x_0 x_1 x_3 x_4 x_6 x_8 x_9 \oplus x_0 x_1 x_3 x_4 x_7 \oplus x_0 x_1 x_3 x_4 x_7 x_8 x_9 \oplus x_0 x_1 x_3 x_4 x_7 x_9 \oplus x_0 x_1 x_3 x_4 x_8 \oplus x_0 x_1 x_3 x_4 x_9 \oplus \\
& x_0 x_1 x_3 x_5 \oplus x_0 x_1 x_3 x_5 x_6 \oplus x_0 x_1 x_3 x_5 x_6 x_7 \oplus x_0 x_1 x_3 x_5 x_6 x_7 x_8 \oplus x_0 x_1 x_3 x_5 x_6 x_7 x_8 x_9 \oplus x_0 x_1 x_3 x_5 x_6 x_8 x_9 \oplus x_0 x_1 x_3 x_5 x_6 x_9 \oplus \\
& x_0 x_1 x_3 x_5 x_7 x_8 \oplus x_0 x_1 x_3 x_5 x_7 x_9 \oplus x_0 x_1 x_3 x_5 x_8 \oplus x_0 x_1 x_3 x_5 x_8 x_9 \oplus x_0 x_1 x_3 x_6 x_7 \oplus x_0 x_1 x_3 x_6 x_7 x_8 x_9 \oplus x_0 x_1 x_3 x_6 x_7 x_9 \oplus \\
& x_0 x_1 x_3 x_6 x_8 \oplus x_0 x_1 x_3 x_6 x_9 \oplus x_0 x_1 x_3 x_7 \oplus x_0 x_1 x_3 x_7 x_8 \oplus x_0 x_1 x_3 x_7 x_8 x_9 \oplus x_0 x_1 x_3 x_8 x_9 \oplus x_0 x_1 x_3 x_9 \oplus x_0 x_1 x_4 \oplus \\
& x_0 x_1 x_4 x_5 x_6 \oplus x_0 x_1 x_4 x_5 x_6 x_7 x_8 \oplus x_0 x_1 x_4 x_5 x_6 x_7 x_9 \oplus x_0 x_1 x_4 x_5 x_6 x_8 \oplus x_0 x_1 x_4 x_5 x_6 x_8 x_9 \oplus x_0 x_1 x_4 x_5 x_7 \oplus x_0 x_1 x_4 x_5 x_7 x_8 x_9 \oplus \\
& x_0 x_1 x_4 x_5 x_7 x_9 \oplus x_0 x_1 x_4 x_5 x_8 \oplus x_0 x_1 x_4 x_5 x_9 \oplus x_0 x_1 x_4 x_6 \oplus x_0 x_1 x_4 x_6 x_7 \oplus x_0 x_1 x_4 x_6 x_7 x_8 \oplus x_0 x_1 x_4 x_6 x_7 x_8 x_9 \oplus \\
& x_0 x_1 x_4 x_6 x_8 x_9 \oplus x_0 x_1 x_4 x_6 x_9 \oplus x_0 x_1 x_4 x_7 x_8 \oplus x_0 x_1 x_4 x_7 x_9 \oplus x_0 x_1 x_4 x_8 \oplus x_0 x_1 x_4 x_8 x_9 \oplus x_0 x_1 x_5 \oplus x_0 x_1 x_5 x_6 x_7 \oplus \\
& x_0 x_1 x_5 x_6 x_7 x_8 x_9 \oplus x_0 x_1 x_5 x_6 x_7 x_9 \oplus x_0 x_1 x_5 x_6 x_8 \oplus x_0 x_1 x_5 x_6 x_9 \oplus x_0 x_1 x_5 x_7 \oplus x_0 x_1 x_5 x_7 x_8 \oplus x_0 x_1 x_5 x_7 x_8 x_9 \oplus \\
& x_0 x_1 x_5 x_8 x_9 \oplus x_0 x_1 x_5 x_9 \oplus x_0 x_1 x_6 \oplus x_0 x_1 x_6 x_7 x_8 \oplus x_0 x_1 x_6 x_7 x_9 \oplus x_0 x_1 x_6 x_8 \oplus x_0 x_1 x_6 x_8 x_9 \oplus x_0 x_1 x_7 \oplus x_0 x_1 x_7 x_8 x_9 \oplus \\
& x_0 x_1 x_7 x_9 \oplus x_0 x_1 x_8 \oplus x_0 x_1 x_9 \oplus x_0 x_2 \oplus x_0 x_2 x_3 \oplus x_0 x_2 x_3 x_4 \oplus x_0 x_2 x_3 x_4 x_5 \oplus x_0 x_2 x_3 x_4 x_5 x_6 \oplus x_0 x_2 x_3 x_4 x_5 x_6 x_7 \oplus \\
& x_0 x_2 x_3 x_4 x_5 x_6 x_7 x_8 \oplus x_0 x_2 x_3 x_4 x_5 x_6 x_7 x_8 x_9 \oplus x_0 x_2 x_3 x_4 x_5 x_6 x_8 x_9 \oplus x_0 x_2 x_3 x_4 x_5 x_6 x_9 \oplus x_0 x_2 x_3 x_4 x_5 x_7 x_8 \oplus x_0 x_2 x_3 x_4 x_5 x_7 x_9 \oplus \\
& x_0 x_2 x_3 x_4 x_5 x_8 \oplus x_0 x_2 x_3 x_4 x_5 x_8 x_9 \oplus x_0 x_2 x_3 x_4 x_6 x_7 \oplus x_0 x_2 x_3 x_4 x_6 x_7 x_8 x_9 \oplus x_0 x_2 x_3 x_4 x_6 x_7 x_9 \oplus x_0 x_2 x_3 x_4 x_6 x_8 \oplus \\
& x_0 x_2 x_3 x_4 x_6 x_9 \oplus x_0 x_2 x_3 x_4 x_7 \oplus x_0 x_2 x_3 x_4 x_7 x_8 \oplus x_0 x_2 x_3 x_4 x_7 x_8 x_9 \oplus x_0 x_2 x_3 x_4 x_8 x_9 \oplus x_0 x_2 x_3 x_4 x_9 \oplus x_0 x_2 x_3 x_5 x_6 \oplus \\
& x_0 x_2 x_3 x_5 x_6 x_7 x_8 \oplus x_0 x_2 x_3 x_5 x_6 x_7 x_9 \oplus x_0 x_2 x_3 x_5 x_6 x_8 \oplus x_0 x_2 x_3 x_5 x_6 x_8 x_9 \oplus x_0 x_2 x_3 x_5 x_7 \oplus x_0 x_2 x_3 x_5 x_7 x_8 x_9 \oplus \\
& x_0 x_2 x_3 x_5 x_7 x_9 \oplus x_0 x_2 x_3 x_5 x_8 \oplus x_0 x_2 x_3 x_5 x_9 \oplus x_0 x_2 x_3 x_6 \oplus x_0 x_2 x_3 x_6 x_7 \oplus x_0 x_2 x_3 x_6 x_7 x_8 \oplus x_0 x_2 x_3 x_6 x_7 x_8 x_9 \oplus \\
& x_0 x_2 x_3 x_6 x_8 x_9 \oplus x_0 x_2 x_3 x_6 x_9 \oplus x_0 x_2 x_3 x_7 x_8 \oplus x_0 x_2 x_3 x_8 \oplus x_0 x_2 x_3 x_8 x_9 \oplus x_0 x_2 x_4 x_5 \oplus x_0 x_2 x_4 x_5 x_6 x_7 \oplus \\
& x_0 x_2 x_4 x_5 x_6 x_7 x_8 x_9 \oplus x_0 x_2 x_4 x_5 x_6 x_7 x_9 \oplus x_0 x_2 x_4 x_5 x_6 x_8 \oplus x_0 x_2 x_4 x_5 x_6 x_9 \oplus x_0 x_2 x_4 x_5 x_7 \oplus x_0 x_2 x_4 x_5 x_7 x_8 \oplus \\
& x_0 x_2 x_4 x_5 x_7 x_8 x_9 \oplus x_0 x_2 x_4 x_5 x_8 x_9 \oplus x_0 x_2 x_4 x_5 x_9 \oplus x_0 x_2 x_4 x_6 \oplus x_0 x_2 x_4 x_6 x_7 x_8 \oplus x_0 x_2 x_4 x_6 x_7 x_9 \oplus x_0 x_2 x_4 x_6 x_8 \oplus \\
& x_0 x_2 x_4 x_6 x_8 x_9 \oplus x_0 x_2 x_4 x_7 \oplus x_0 x_2 x_4 x_7 x_8 x_9 \oplus x_0 x_2 x_4 x_7 x_9 \oplus x_0 x_2 x_4 x_8 \oplus x_0 x_2 x_4 x_8 x_9 \oplus x_0 x_2 x_4 x_9 \oplus x_0 x_2 x_5 \oplus x_0 x_2 x_5 x_6 \oplus \\
& x_0 x_2 x_5 x_6 x_7 \oplus x_0 x_2 x_5 x_6 x_7 x_8 \oplus x_0 x_2 x_5 x_6 x_7 x_8 x_9 \oplus x_0 x_2 x_5 x_6 x_8 x_9 \oplus x_0 x_2 x_5 x_6 x_9 \oplus x_0 x_2 x_5 x_7 x_8 \oplus x_0 x_2 x_5 x_7 x_8 x_9 \oplus \\
& x_0 x_2 x_5 x_8 \oplus x_0 x_2 x_5 x_8 x_9 \oplus x_0 x_2 x_6 x_7 \oplus x_0 x_2 x_6 x_7 x_8 x_9 \oplus x_0 x_2 x_6 x_7 x_9 \oplus x_0 x_2 x_6 x_8 \oplus x_0 x_2 x_6 x_8 x_9 \oplus x_0 x_2 x_6 x_9 \oplus x_0 x_2 x_7 \oplus \\
& x_0 x_2 x_7 x_8 \oplus x_0 x_2 x_7 x_8 x_9 \oplus x_0 x_2 x_8 x_9 \oplus x_0 x_2 x_9 \oplus x_0 x_3 x_4 \oplus x_0 x_3 x_4 x_5 x_6 \oplus x_0 x_3 x_4 x_5 x_6 x_7 x_8 \oplus x_0 x_3 x_4 x_5 x_6 x_7 x_9 \oplus \\
& x_0 x_3 x_4 x_5 x_6 x_8 \oplus x_0 x_3 x_4 x_5 x_6 x_8 x_9 \oplus x_0 x_3 x_4 x_5 x_7 \oplus x_0 x_3 x_4 x_5 x_7 x_8 x_9 \oplus x_0 x_3 x_4 x_5 x_7 x_9 \oplus x_0 x_3 x_4 x_5 x_8 \oplus x_0 x_3 x_4 x_5 x_8 x_9 \oplus \\
& x_0 x_3 x_4 x_6 \oplus x_0 x_3 x_4 x_6 x_7 \oplus x_0 x_3 x_4 x_6 x_7 x_8 \oplus x_0 x_3 x_4 x_6 x_7 x_8 x_9 \oplus x_0 x_3 x_4 x_6 x_8 \oplus x_0 x_3 x_4 x_6 x_8 x_9 \oplus x_0 x_3 x_4 x_6 x_9 \oplus x_0 x_3 x_4 x_7 x_8 \oplus \\
& x_0 x_3 x_4 x_7 x_9 \oplus x_0 x_3 x_4 x_8 \oplus x_0 x_3 x_4 x_8 x_9 \oplus x_0 x_3 x_5 \oplus x_0 x_3 x_5 x_6 x_7 \oplus x_0 x_3 x_5 x_6 x_7 x_8 x_9 \oplus x_0 x_3 x_5 x_6 x_7 x_9 \oplus x_0 x_3 x_5 x_6 x_8 \oplus \\
& x_0 x_3 x_5 x_6 x_9 \oplus x_0 x_3 x_5 x_7 \oplus x_0 x_3 x_5 x_7 x_8 \oplus x_0 x_3 x_5 x_7 x_8 x_9 \oplus x_0 x_3 x_5 x_8 x_9 \oplus x_0 x_3 x_5 x_9 \oplus x_0 x_3 x_6 \oplus x_0 x_3 x_6 x_7 x_8 \oplus \\
& x_0 x_3 x_6 x_7 x_9 \oplus x_0 x_3 x_6 x_8 \oplus x_0 x_3 x_6 x_8 x_9 \oplus x_0 x_3 x_7 \oplus x_0 x_3 x_7 x_8 x_9 \oplus x_0 x_3 x_7 x_9 \oplus x_0 x_3 x_8 \oplus x_0 x_3 x_9 \oplus x_0 x_4 \oplus x_0 x_4 x_5 \oplus
\end{aligned}$$

$$\begin{aligned}
& 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
\end{aligned}$$

$$\begin{aligned}
& x_0x_1 \oplus x_0x_1x_2x_3 \oplus x_0x_1x_2x_3x_4x_5 \oplus x_0x_1x_2x_3x_4x_5x_6x_7 \oplus x_0x_1x_2x_3x_4x_5x_6x_7x_8x_9 \oplus x_0x_1x_2x_3x_4x_5x_6x_7x_9 \oplus \\
& x_0x_1x_2x_3x_4x_5x_6x_8 \oplus x_0x_1x_2x_3x_4x_5x_6x_9 \oplus x_0x_1x_2x_3x_4x_5x_7 \oplus x_0x_1x_2x_3x_4x_5x_7x_8 \oplus x_0x_1x_2x_3x_4x_5x_7x_8x_9 \oplus \\
& x_0x_1x_2x_3x_4x_5x_8x_9 \oplus x_0x_1x_2x_3x_4x_5x_9 \oplus x_0x_1x_2x_3x_4x_6 \oplus x_0x_1x_2x_3x_4x_6x_7x_8 \oplus x_0x_1x_2x_3x_4x_6x_7x_9 \oplus x_0x_1x_2x_3x_4x_6x_8 \oplus \\
& x_0x_1x_2x_3x_4x_6x_8x_9 \oplus x_0x_1x_2x_3x_4x_7 \oplus x_0x_1x_2x_3x_4x_7x_8x_9 \oplus x_0x_1x_2x_3x_4x_7x_9 \oplus x_0x_1x_2x_3x_4x_8 \oplus x_0x_1x_2x_3x_4x_9 \oplus \\
& x_0x_1x_2x_3x_5 \oplus x_0x_1x_2x_3x_5x_6 \oplus x_0x_1x_2x_3x_5x_6x_7 \oplus x_0x_1x_2x_3x_5x_6x_7x_8 \oplus x_0x_1x_2x_3x_5x_6x_7x_8x_9 \oplus x_0x_1x_2x_3x_5x_6x_8x_9 \oplus \\
& x_0x_1x_2x_3x_5x_6x_9 \oplus x_0x_1x_2x_3x_5x_7x_8 \oplus x_0x_1x_2x_3x_5x_7x_9 \oplus x_0x_1x_2x_3x_5x_8 \oplus x_0x_1x_2x_3x_5x_8x_9 \oplus x_0x_1x_2x_3x_5x_6x_7 \oplus
\end{aligned}$$

465 $x_0x_1x_2x_3x_6x_7x_8x_9 \oplus x_0x_1x_2x_3x_6x_7x_9 \oplus x_0x_1x_2x_3x_6x_8 \oplus x_0x_1x_2x_3x_6x_9 \oplus x_0x_1x_2x_3x_7 \oplus x_0x_1x_2x_3x_7x_8 \oplus$
466 $x_0x_1x_2x_3x_7x_8x_9 \oplus x_0x_1x_2x_3x_8x_9 \oplus x_0x_1x_2x_3x_9 \oplus x_0x_1x_2x_4 \oplus x_0x_1x_2x_4x_5x_6 \oplus x_0x_1x_2x_4x_5x_6x_7x_8 \oplus x_0x_1x_2x_4x_5x_6x_7x_9 \oplus$
467 $x_0x_1x_2x_4x_5x_6x_8 \oplus x_0x_1x_2x_4x_5x_6x_8x_9 \oplus x_0x_1x_2x_4x_5x_7 \oplus x_0x_1x_2x_4x_5x_7x_8x_9 \oplus x_0x_1x_2x_4x_5x_7x_9 \oplus x_0x_1x_2x_4x_5x_8 \oplus$
468 $x_0x_1x_2x_4x_5x_9 \oplus x_0x_1x_2x_4x_6 \oplus x_0x_1x_2x_4x_6x_7 \oplus x_0x_1x_2x_4x_6x_7x_8 \oplus x_0x_1x_2x_4x_6x_7x_8x_9 \oplus x_0x_1x_2x_4x_6x_8x_9 \oplus$
469 $x_0x_1x_2x_4x_6x_9 \oplus x_0x_1x_2x_4x_7x_8 \oplus x_0x_1x_2x_4x_7x_9 \oplus x_0x_1x_2x_4x_8 \oplus x_0x_1x_2x_4x_8x_9 \oplus x_0x_1x_2x_5 \oplus x_0x_1x_2x_5x_6x_7 \oplus$
470 $x_0x_1x_2x_5x_6x_7x_8x_9 \oplus x_0x_1x_2x_5x_6x_7x_9 \oplus x_0x_1x_2x_5x_6x_8 \oplus x_0x_1x_2x_5x_6x_9 \oplus x_0x_1x_2x_5x_7 \oplus x_0x_1x_2x_5x_7x_8 \oplus$
471 $x_0x_1x_2x_5x_7x_8x_9 \oplus x_0x_1x_2x_5x_8x_9 \oplus x_0x_1x_2x_5x_9 \oplus x_0x_1x_2x_6 \oplus x_0x_1x_2x_6x_7x_8 \oplus x_0x_1x_2x_6x_7x_9 \oplus x_0x_1x_2x_6x_8 \oplus$
472 $x_0x_1x_2x_6x_8x_9 \oplus x_0x_1x_2x_7 \oplus x_0x_1x_2x_7x_8x_9 \oplus x_0x_1x_2x_7x_9 \oplus x_0x_1x_2x_8 \oplus x_0x_1x_2x_9 \oplus x_0x_1x_3 \oplus x_0x_1x_3x_4 \oplus$
473 $x_0x_1x_3x_4x_5 \oplus x_0x_1x_3x_4x_5x_6 \oplus x_0x_1x_3x_4x_5x_6x_7 \oplus x_0x_1x_3x_4x_5x_6x_7x_8 \oplus x_0x_1x_3x_4x_5x_6x_7x_8x_9 \oplus x_0x_1x_3x_4x_5x_6x_8x_9 \oplus$
474 $x_0x_1x_3x_4x_5x_6x_9 \oplus x_0x_1x_3x_4x_5x_7x_8 \oplus x_0x_1x_3x_4x_5x_7x_9 \oplus x_0x_1x_3x_4x_5x_8 \oplus x_0x_1x_3x_4x_5x_8x_9 \oplus x_0x_1x_3x_4x_6x_7 \oplus$
475 $x_0x_1x_3x_4x_6x_7x_8x_9 \oplus x_0x_1x_3x_4x_6x_7x_9 \oplus x_0x_1x_3x_4x_6x_8 \oplus x_0x_1x_3x_4x_6x_9 \oplus x_0x_1x_3x_4x_7 \oplus x_0x_1x_3x_4x_7x_8 \oplus$
476 $x_0x_1x_3x_4x_7x_8x_9 \oplus x_0x_1x_3x_4x_8x_9 \oplus x_0x_1x_3x_4x_9 \oplus x_0x_1x_3x_5x_6 \oplus x_0x_1x_3x_5x_6x_7x_8 \oplus x_0x_1x_3x_5x_6x_7x_9 \oplus x_0x_1x_3x_5x_6x_8 \oplus$
477 $x_0x_1x_3x_5x_6x_8x_9 \oplus x_0x_1x_3x_5x_7 \oplus x_0x_1x_3x_5x_7x_8x_9 \oplus x_0x_1x_3x_5x_7x_9 \oplus x_0x_1x_3x_5x_8 \oplus x_0x_1x_3x_5x_9 \oplus x_0x_1x_3x_6 \oplus$
478 $x_0x_1x_3x_6x_7 \oplus x_0x_1x_3x_6x_7x_8 \oplus x_0x_1x_3x_6x_7x_8x_9 \oplus x_0x_1x_3x_6x_8x_9 \oplus x_0x_1x_3x_6x_9 \oplus x_0x_1x_3x_7x_8 \oplus x_0x_1x_3x_7x_9 \oplus$
479 $x_0x_1x_3x_8 \oplus x_0x_1x_3x_8x_9 \oplus x_0x_1x_4x_5 \oplus x_0x_1x_4x_5x_6x_7 \oplus x_0x_1x_4x_5x_6x_7x_8x_9 \oplus x_0x_1x_4x_5x_6x_7x_9 \oplus x_0x_1x_4x_5x_6x_8 \oplus$
480 $x_0x_1x_4x_5x_6x_9 \oplus x_0x_1x_4x_5x_7 \oplus x_0x_1x_4x_5x_7x_8 \oplus x_0x_1x_4x_5x_7x_8x_9 \oplus x_0x_1x_4x_5x_8x_9 \oplus x_0x_1x_4x_5x_9 \oplus x_0x_1x_4x_6 \oplus$
481 $x_0x_1x_4x_6x_7x_8 \oplus x_0x_1x_4x_6x_7x_9 \oplus x_0x_1x_4x_6x_8 \oplus x_0x_1x_4x_6x_8x_9 \oplus x_0x_1x_4x_7 \oplus x_0x_1x_4x_7x_8x_9 \oplus x_0x_1x_4x_7x_9 \oplus$
482 $x_0x_1x_4x_8 \oplus x_0x_1x_4x_9 \oplus x_0x_1x_5 \oplus x_0x_1x_5x_6 \oplus x_0x_1x_5x_6x_7 \oplus x_0x_1x_5x_6x_7x_8 \oplus x_0x_1x_5x_6x_7x_8x_9 \oplus x_0x_1x_5x_6x_8x_9 \oplus$
483 $x_0x_1x_5x_6x_9 \oplus x_0x_1x_5x_7x_8 \oplus x_0x_1x_5x_7x_9 \oplus x_0x_1x_5x_8 \oplus x_0x_1x_5x_8x_9 \oplus x_0x_1x_6x_7 \oplus x_0x_1x_6x_7x_8x_9 \oplus x_0x_1x_6x_7x_9 \oplus$
484 $x_0x_1x_6x_8 \oplus x_0x_1x_6x_9 \oplus x_0x_1x_7 \oplus x_0x_1x_7x_8 \oplus x_0x_1x_7x_8x_9 \oplus x_0x_1x_8x_9 \oplus x_0x_1x_9 \oplus x_0x_2 \oplus x_0x_2x_3x_4 \oplus x_0x_2x_3x_4x_5x_6 \oplus$
485 $x_0x_2x_3x_4x_5x_6x_7x_8 \oplus x_0x_2x_3x_4x_5x_6x_7x_9 \oplus x_0x_2x_3x_4x_5x_6x_8 \oplus x_0x_2x_3x_4x_5x_6x_8x_9 \oplus x_0x_2x_3x_4x_5x_7 \oplus x_0x_2x_3x_4x_5x_7x_8x_9 \oplus$
486 $x_0x_2x_3x_4x_5x_7x_9 \oplus x_0x_2x_3x_4x_5x_8 \oplus x_0x_2x_3x_4x_5x_9 \oplus x_0x_2x_3x_4x_6 \oplus x_0x_2x_3x_4x_6x_7 \oplus x_0x_2x_3x_4x_6x_7x_8 \oplus x_0x_2x_3x_4x_6x_7x_8x_9 \oplus$
487 $x_0x_2x_3x_4x_6x_8x_9 \oplus x_0x_2x_3x_4x_6x_9 \oplus x_0x_2x_3x_4x_7x_8 \oplus x_0x_2x_3x_4x_7x_9 \oplus x_0x_2x_3x_4x_8 \oplus x_0x_2x_3x_4x_8x_9 \oplus x_0x_2x_3x_5 \oplus$
488 $x_0x_2x_3x_5x_6x_7 \oplus x_0x_2x_3x_5x_6x_7x_8x_9 \oplus x_0x_2x_3x_5x_6x_7x_9 \oplus x_0x_2x_3x_5x_6x_8 \oplus x_0x_2x_3x_5x_6x_9 \oplus x_0x_2x_3x_5x_7 \oplus$
489 $x_0x_2x_3x_5x_7x_8 \oplus x_0x_2x_3x_5x_7x_8x_9 \oplus x_0x_2x_3x_5x_8x_9 \oplus x_0x_2x_3x_5x_9 \oplus x_0x_2x_3x_6 \oplus x_0x_2x_3x_6x_7x_8 \oplus x_0x_2x_3x_6x_7x_9 \oplus$
490 $x_0x_2x_3x_6x_8 \oplus x_0x_2x_3x_6x_8x_9 \oplus x_0x_2x_3x_7 \oplus x_0x_2x_3x_7x_8x_9 \oplus x_0x_2x_3x_7x_9 \oplus x_0x_2x_3x_8 \oplus x_0x_2x_3x_9 \oplus x_0x_2x_4 \oplus$
491 $x_0x_2x_4x_5 \oplus x_0x_2x_4x_5x_6 \oplus x_0x_2x_4x_5x_6x_7 \oplus x_0x_2x_4x_5x_6x_7x_8 \oplus x_0x_2x_4x_5x_6x_7x_8x_9 \oplus x_0x_2x_4x_5x_6x_8x_9 \oplus x_0x_2x_4x_5x_6x_9 \oplus$
492 $x_0x_2x_4x_5x_7x_8 \oplus$

517 $x_1x_2x_5x_6x_7 \oplus x_1x_2x_5x_6x_7x_8 \oplus x_1x_2x_5x_6x_7x_8x_9 \oplus x_1x_2x_5x_6x_8x_9 \oplus x_1x_2x_5x_6x_9 \oplus x_1x_2x_5x_7x_8 \oplus x_1x_2x_5x_7x_9 \oplus$
518 $x_1x_2x_5x_8 \oplus x_1x_2x_5x_8x_9 \oplus x_1x_2x_6x_7 \oplus x_1x_2x_6x_7x_8x_9 \oplus x_1x_2x_6x_7x_9 \oplus x_1x_2x_6x_8 \oplus x_1x_2x_6x_9 \oplus x_1x_2x_7 \oplus$
519 $x_1x_2x_7x_8 \oplus x_1x_2x_7x_8x_9 \oplus x_1x_2x_8x_9 \oplus x_1x_2x_9 \oplus x_1x_3x_4 \oplus x_1x_3x_4x_5x_6 \oplus x_1x_3x_4x_5x_6x_7x_8 \oplus x_1x_3x_4x_5x_6x_7x_9 \oplus$
520 $x_1x_3x_4x_5x_6x_8 \oplus x_1x_3x_4x_5x_6x_8x_9 \oplus x_1x_3x_4x_5x_7 \oplus x_1x_3x_4x_5x_7x_8x_9 \oplus x_1x_3x_4x_5x_7x_9 \oplus x_1x_3x_4x_5x_8 \oplus x_1x_3x_4x_5x_9 \oplus$
521 $x_1x_3x_4x_6 \oplus x_1x_3x_4x_6x_7 \oplus x_1x_3x_4x_6x_7x_8 \oplus x_1x_3x_4x_6x_7x_8x_9 \oplus x_1x_3x_4x_6x_8x_9 \oplus x_1x_3x_4x_6x_9 \oplus x_1x_3x_4x_7x_8 \oplus$
522 $x_1x_3x_4x_7x_9 \oplus x_1x_3x_4x_8 \oplus x_1x_3x_4x_8x_9 \oplus x_1x_3x_5 \oplus x_1x_3x_5x_6x_7 \oplus x_1x_3x_5x_6x_7x_8x_9 \oplus x_1x_3x_5x_6x_7x_9 \oplus x_1x_3x_5x_6x_8 \oplus$
523 $x_1x_3x_5x_6x_9 \oplus x_1x_3x_5x_7 \oplus x_1x_3x_5x_7x_8 \oplus x_1x_3x_5x_7x_8x_9 \oplus x_1x_3x_5x_8x_9 \oplus x_1x_3x_5x_9 \oplus x_1x_3x_6 \oplus x_1x_3x_6x_7x_8 \oplus$
524 $x_1x_3x_6x_7x_9 \oplus x_1x_3x_6x_8 \oplus x_1x_3x_6x_8x_9 \oplus x_1x_3x_7 \oplus x_1x_3x_7x_8x_9 \oplus x_1x_3x_7x_9 \oplus x_1x_3x_8 \oplus x_1x_3x_9 \oplus x_1x_4 \oplus x_1x_4x_5 \oplus$
525 $x_1x_4x_5x_6 \oplus x_1x_4x_5x_6x_7 \oplus x_1x_4x_5x_6x_7x_8 \oplus x_1x_4x_5x_6x_7x_8x_9 \oplus x_1x_4x_5x_6x_8x_9 \oplus x_1x_4x_5x_6x_9 \oplus x_1x_4x_5x_7x_8 \oplus$
526 $x_1x_4x_5x_7x_9 \oplus x_1x_4x_5x_8 \oplus x_1x_4x_5x_8x_9 \oplus x_1x_4x_6x_7 \oplus x_1x_4x_6x_7x_8x_9 \oplus x_1x_4x_6x_7x_9 \oplus x_1x_4x_6x_8 \oplus x_1x_4x_6x_9 \oplus$
527 $x_1x_4x_7 \oplus x_1x_4x_7x_8 \oplus x_1x_4x_7x_8x_9 \oplus x_1x_4x_8x_9 \oplus x_1x_4x_9 \oplus x_1x_5x_6 \oplus x_1x_5x_6x_7x_8 \oplus x_1x_5x_6x_7x_9 \oplus x_1x_5x_6x_8 \oplus$
528 $x_1x_5x_6x_8x_9 \oplus x_1x_5x_7 \oplus x_1x_5x_7x_8x_9 \oplus x_1x_5x_7x_9 \oplus x_1x_5x_8 \oplus x_1x_5x_9 \oplus x_1x_6 \oplus x_1x_6x_7 \oplus x_1x_6x_7x_8 \oplus x_1x_6x_7x_8x_9 \oplus$
529 $x_1x_6x_8x_9 \oplus x_1x_6x_9 \oplus x_1x_7x_8 \oplus x_1x_7x_9 \oplus x_1x_8 \oplus x_1x_8x_9 \oplus x_2x_3 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_4x_5x_6x_7 \oplus x_2x_3x_4x_5x_6x_7x_8x_9 \oplus$
530 $x_2x_3x_4x_5x_6x_7x_9 \oplus x_2x_3x_4x_5x_6x_8 \oplus x_2x_3x_4x_5x_6x_9 \oplus x_2x_3x_4x_5x_7 \oplus x_2x_3x_4x_5x_7x_8 \oplus x_2x_3x_4x_5x_7x_8x_9 \oplus x_2x_3x_4x_5x_8x_9 \oplus$
531 $x_2x_3x_4x_5x_9 \oplus x_2x_3x_4x_6 \oplus x_2x_3x_4x_6x_7x_8 \oplus x_2x_3x_4x_6x_7x_9 \oplus x_2x_3x_4x_6x_8 \oplus x_2x_3x_4x_6x_8x_9 \oplus x_2x_3x_4x_7 \oplus x_2x_3x_4x_7x_8x_9 \oplus$
532 $x_2x_3x_4x_7x_9 \oplus x_2x_3x_4x_8 \oplus x_2x_3x_4x_9 \oplus x_2x_3x_5 \oplus x_2x_3x_5x_6 \oplus x_2x_3x_5x_6x_7 \oplus x_2x_3x_5x_6x_7x_8 \oplus x_2x_3x_5x_6x_7x_8x_9 \oplus$
533 $x_2x_3x_5x_6x_8x_9 \oplus x_2x_3x_5x_6x_9 \oplus x_2x_3x_5x_7x_8 \oplus x_2x_3x_5x_7x_9 \oplus x_2x_3x_5x_8 \oplus x_2x_3x_5x_8x_9 \oplus x_2x_3x_6x_7 \oplus x_2x_3x_6x_7x_8x_9 \oplus$
534 $x_2x_3x_6x_7x_9 \oplus x_2x_3x_6x_8 \oplus x_2x_3x_6x_9 \oplus x_2x_3x_7 \oplus x_2x_3x_7x_8 \oplus x_2x_3x_7x_8x_9 \oplus x_2x_3x_8x_9 \oplus x_2x_3x_9 \oplus x_2x_4 \oplus x_2x_4x_5x_6 \oplus$
535 $x_2x_4x_5x_6x_7x_8 \oplus x_2x_4x_5x_6x_7x_9 \oplus x_2x_4x_5x_6x_8 \oplus x_2x_4x_5x_6x_8x_9 \oplus x_2x_4x_5x_7 \oplus x_2x_4x_5x_7x_8x_9 \oplus x_2x_4x_5x_7x_9 \oplus$
536 $x_2x_4x_5x_8 \oplus x_2x_4x_5x_9 \oplus x_2x_4x_6 \oplus x_2x_4x_6x_7 \oplus x_2x_4x_6x_7x_8 \oplus x_2x_4x_6x_7x_8x_9 \oplus x_2x_4x_6x_8x_9 \oplus x_2x_4x_6x_9 \oplus x_2x_4x_7x_8 \oplus$
537 $x_2x_4x_7x_9 \oplus x_2x_4x_8 \oplus x_2x_4x_8x_9 \oplus x_2x_5 \oplus x_2x_5x_6x_7 \oplus x_2x_5x_6x_7x_8x_9 \oplus x_2x_5x_6x_7x_9 \oplus x_2x_5x_6x_8 \oplus x_2x_5x_6x_9 \oplus$
538 $x_2x_5x_7 \oplus x_2x_5x_7x_8 \oplus x_2x_5x_7x_8x_9 \oplus x_2x_5x_8x_9 \oplus x_2x_5x_9 \oplus x_2x_6 \oplus x_2x_6x_7x_8 \oplus x_2x_6x_7x_9 \oplus x_2x_6x_8 \oplus x_2x_6x_8x_9 \oplus$
539 $x_2x_7 \oplus x_2x_7x_8x_9 \oplus x_2x_7x_9 \oplus x_2x_8 \oplus x_2x_9 \oplus x_3 \oplus x_3x_4 \oplus x_3x_4x_5 \oplus x_3x_4x_5x_6 \oplus x_3x_4x_5x_6x_7 \oplus x_3x_4x_5x_6x_7x_8 \oplus$
540 $x_3x_4x_5x_6x_7x_8x_9 \oplus x_3x_4x_5x_6x_8x_9 \oplus x_3x_4x_5x_6x_9 \oplus x_3x_4x_5x_7x_8 \oplus x_3x_4x_5x_7x_9 \oplus x_3x_4x_5x_8 \oplus x_3x_4x_5x_8x_9 \oplus$
541 $x_3x_4x_6x_7 \oplus x_3x_4x_6x_7x_8x_9 \oplus x_3x_4x_6x_7x_9 \oplus x_3x_4x_6x_8 \oplus x_3x_4x_6x_9 \oplus x_3x_4x_7 \oplus x_3x_4x_7x_8 \oplus x_3x_4x_7x_8x_9 \oplus x_3x_4x_8x_9 \oplus$
542 $x_3x_4x_9 \oplus x_3x_5x_6 \oplus x_3x_5x_6x_7x_8 \oplus x_3x_5x_6x_7x_9 \oplus x_3x_5x_6x_8 \oplus x_3x_5x_6x_8x_9 \oplus x_3x_5x_7 \oplus x_3x_5x_7x_8x_9 \oplus x_3x_5x_7x_9 \oplus$
543 $x_3x_5x_8 \oplus x_3x_5x_9 \oplus x_3x_6 \oplus x_3x_6x_7 \oplus x_3x_6x_7x_8 \oplus x_3x_6x_7x_8x_9 \oplus x_3x_6x_8x_9 \oplus x_3x_6x_9 \oplus x_3x_7x_8 \oplus x_3x_7x_9 \oplus x_3x_8 \oplus$
544 $x_3x_8x_9 \oplus x_4x_5 \oplus x_4x_5x_6x_7 \oplus x_4x_5x_6x_7x_8x_9 \oplus x_4$

$x_0x_1x_3x_8 \oplus x_0x_1x_3x_9 \oplus x_0x_1x_4 \oplus x_0x_1x_4x_5 \oplus x_0x_1x_4x_5x_6 \oplus x_0x_1x_4x_5x_6x_7 \oplus x_0x_1x_4x_5x_6x_7x_8 \oplus x_0x_1x_4x_5x_6x_7x_8x_9 \oplus$
 $x_0x_1x_4x_5x_6x_8x_9 \oplus x_0x_1x_4x_5x_6x_9 \oplus x_0x_1x_4x_5x_7x_8 \oplus x_0x_1x_4x_5x_7x_9 \oplus x_0x_1x_4x_5x_8 \oplus x_0x_1x_4x_5x_8x_9 \oplus x_0x_1x_4x_6x_7 \oplus$
 $x_0x_1x_4x_6x_7x_8x_9 \oplus x_0x_1x_4x_6x_7x_9 \oplus x_0x_1x_4x_6x_8 \oplus x_0x_1x_4x_6x_9 \oplus x_0x_1x_4x_7 \oplus x_0x_1x_4x_7x_8 \oplus x_0x_1x_4x_7x_8x_9 \oplus$
 $x_0x_1x_4x_8x_9 \oplus x_0x_1x_4x_9 \oplus x_0x_1x_5x_6 \oplus x_0x_1x_5x_6x_7x_8 \oplus x_0x_1x_5x_6x_7x_9 \oplus x_0x_1x_5x_6x_8 \oplus x_0x_1x_5x_6x_8x_9 \oplus x_0x_1x_5x_7 \oplus$
 $x_0x_1x_5x_7x_8x_9 \oplus x_0x_1x_5x_7x_9 \oplus x_0x_1x_5x_8 \oplus x_0x_1x_5x_9 \oplus x_0x_1x_6 \oplus x_0x_1x_6x_7 \oplus x_0x_1x_6x_7x_8 \oplus x_0x_1x_6x_7x_8x_9 \oplus$
 $x_0x_1x_6x_8x_9 \oplus x_0x_1x_6x_9 \oplus x_0x_1x_7x_8 \oplus x_0x_1x_7x_9 \oplus x_0x_1x_8 \oplus x_0x_1x_8x_9 \oplus x_0x_2x_3 \oplus x_0x_2x_3x_4x_5 \oplus x_0x_2x_3x_4x_5x_6x_7 \oplus$
 $x_0x_2x_3x_4x_5x_6x_7x_8x_9 \oplus x_0x_2x_3x_4x_5x_6x_7x_9 \oplus x_0x_2x_3x_4x_5x_6x_8 \oplus x_0x_2x_3x_4x_5x_6x_9 \oplus x_0x_2x_3x_4x_5x_7 \oplus x_0x_2x_3x_4x_5x_7x_8 \oplus$
 $x_0x_2x_3x_4x_5x_7x_8x_9 \oplus x_0x_2x_3x_4x_5x_8x_9 \oplus x_0x_2x_3x_4x_5x_9 \oplus x_0x_2x_3x_4x_6 \oplus x_0x_2x_3x_4x_6x_7x_8 \oplus x_0x_2x_3x_4x_6x_7x_9 \oplus$
 $x_0x_2x_3x_4x_6x_8 \oplus x_0x_2x_3x_4x_6x_8x_9 \oplus x_0x_2x_3x_4x_7 \oplus x_0x_2x_3x_4x_7x_8x_9 \oplus x_0x_2x_3x_4x_7x_9 \oplus x_0x_2x_3x_4x_8 \oplus x_0x_2x_3x_4x_9 \oplus$
 $x_0x_2x_3x_5 \oplus x_0x_2x_3x_5x_6 \oplus x_0x_2x_3x_5x_6x_7 \oplus x_0x_2x_3x_5x_6x_7x_8 \oplus x_0x_2x_3x_5x_6x_7x_8x_9 \oplus x_0x_2x_3x_5x_6x_8x_9 \oplus x_0x_2x_3x_5x_6x_9 \oplus$
 $x_0x_2x_3x_5x_7x_8 \oplus x_0x_2x_3x_5x_7x_9 \oplus x_0x_2x_3x_5x_8 \oplus x_0x_2x_3x_5x_8x_9 \oplus x_0x_2x_3x_6x_7 \oplus x_0x_2x_3x_6x_7x_8x_9 \oplus x_0x_2x_3x_6x_7x_9 \oplus$
 $x_0x_2x_3x_6x_8 \oplus x_0x_2x_3x_6x_9 \oplus x_0x_2x_3x_7 \oplus x_0x_2x_3x_7x_8 \oplus x_0x_2x_3x_7x_8x_9 \oplus x_0x_2x_3x_8x_9 \oplus x_0x_2x_3x_9 \oplus x_0x_2x_4 \oplus$
 $x_0x_2x_4x_5x_6 \oplus x_0x_2x_4x_5x_6x_7x_8 \oplus x_0x_2x_4x_5x_6x_7x_9 \oplus x_0x_2x_4x_5x_6x_8 \oplus x_0x_2x_4x_5x_6x_8x_9 \oplus x_0x_2x_4x_5x_7 \oplus x_0x_2x_4x_5x_7x_8x_9 \oplus$
 $x_0x_2x_4x_5x_7x_9 \oplus x_0x_2x_4x_5x_8 \oplus x_0x_2x_4x_5x_9 \oplus x_0x_2x_4x_6 \oplus x_0x_2x_4x_6x_7 \oplus x_0x_2x_4x_6x_7x_8 \oplus x_0x_2x_4x_6x_7x_8x_9 \oplus$
 $x_0x_2x_4x_6x_8x_9 \oplus x_0x_2x_4x_6x_9 \oplus x_0x_2x_4x_7x_8 \oplus x_0x_2x_4x_7x_9 \oplus x_0x_2x_4x_8 \oplus x_0x_2x_4x_8x_9 \oplus x_0x_2x_5 \oplus x_0x_2x_5x_6x_7 \oplus$
 $x_0x_2x_5x_6x_7x_8x_9 \oplus x_0x_2x_5x_6x_7x_9 \oplus x_0x_2x_5x_6x_8 \oplus x_0x_2x_5x_6x_9 \oplus x_0x_2x_5x_7 \oplus x_0x_2x_5x_7x_8 \oplus x_0x_2x_5x_7x_8x_9 \oplus$
 $x_0x_2x_5x_8x_9 \oplus x_0x_2x_5x_9 \oplus x_0x_2x_6 \oplus x_0x_2x_6x_7x_8 \oplus x_0x_2x_6x_7x_9 \oplus x_0x_2x_6x_8 \oplus x_0x_2x_6x_8x_9 \oplus x_0x_2x_7 \oplus x_0x_2x_7x_8x_9 \oplus$
 $x_0x_2x_7x_9 \oplus x_0x_2x_8 \oplus x_0x_2x_9 \oplus x_0x_3 \oplus x_0x_3x_4 \oplus x_0x_3x_4x_5 \oplus x_0x_3x_4x_5x_6 \oplus x_0x_3x_4x_5x_6x_7 \oplus x_0x_3x_4x_5x_6x_7x_8 \oplus$
 $x_0x_3x_4x_5x_6x_7x_8x_9 \oplus x_0x_3x_4x_5x_6x_8x_9 \oplus x_0x_3x_4x_5x_6x_9 \oplus x_0x_3x_4x_5x_7x_8 \oplus x_0x_3x_4x_5x_7x_9 \oplus x_0x_3x_4x_5x_8 \oplus$
 $x_0x_3x_4x_5x_8x_9 \oplus x_0x_3x_4x_6x_7 \oplus x_0x_3x_4x_6x_7x_8x_9 \oplus x_0x_3x_4x_6x_7x_9 \oplus x_0x_3x_4x_6x_8 \oplus x_0x_3x_4x_6x_9 \oplus x_0x_3x_4x_7 \oplus$
 $x_0x_3x_4x_7x_8 \oplus x_0x_3x_4x_7x_8x_9 \oplus x_0x_3x_4x_8x_9 \oplus x_0x_3x_4x_9 \oplus x_0x_3x_5x_6 \oplus x_0x_3x_5x_6x_7x_8 \oplus x_0x_3x_5x_6x_7x_9 \oplus x_0x_3x_5x_6x_8 \oplus$
 $x_0x_3x_5x_6x_8x_9 \oplus x_0x_3x_5x_7 \oplus x_0x_3x_5x_7x_8x_9 \oplus x_0x_3x_5x_7x_9 \oplus x_0x_3x_5x_8 \oplus x_0x_3x_5x_9 \oplus x_0x_3x_6 \oplus x_0x_3x_6x_7 \oplus$
 $x_0x_3x_6x_7x_8 \oplus x_0x_3x_6x_7x_8x_9 \oplus x_0x_3x_6x_8x_9 \oplus x_0x_3x_6x_9 \oplus x_0x_3x_7x_8 \oplus x_0x_3x_7x_9 \oplus x_0x_3x_8 \oplus x_0x_3x_8x_9 \oplus x_0x_4x_5 \oplus$
 $x_0x_4x_5x_6x_7 \oplus x_0x_4x_5x_6x_7x_8x_9 \oplus x_0x_4x_5x_6x_7x_9 \oplus x_0x_4x_5x_6x_8 \oplus x_0x_4x_5x_6x_9 \oplus x_0x_4x_5x_7 \oplus x_0x_4x_5x_7x_8 \oplus$
 $x_0x_4x_5x_7x_8x_9 \oplus x_0x_4x_5x_8x_9 \oplus x_0x_4x_5x_9 \oplus x_0x_4x_6 \oplus x_0x_4x_6x_7x_8 \oplus x_0x_4x_6x_7x_9 \oplus x_0x_4x_6x_8 \oplus x_0x_4x_6x_8x_9 \oplus$
 $x_0x_4x_7 \oplus x_0x_4x_7x_8x_9 \oplus x_0x_4x_7x_9 \oplus x_0x_4x_8 \oplus x_0x_4x_9 \oplus x_0x_5 \oplus x_0x_5x_6 \oplus x_0x_5x_6x_7 \oplus x_0x_5x_6x_7x_8 \oplus x_0x_5x_6x_7x_8x_9 \oplus$
 $x_0x_5x_6x_8x_9 \oplus x_0x_5x_6x_9 \oplus x_0x_5x_7x_8 \oplus x_0x_5x_7x_9 \oplus x_0x_5x_8 \oplus x_0x_5x_8x_9 \oplus x_0x_6x_7 \oplus x_0x_6x_7x_8x_9 \oplus x_0x_6x_7x_9 \oplus$
 $x_0x_6x_8 \oplus x_0x_6x_9 \oplus x_0x_7 \oplus x_0x_7x_8 \oplus x_0x_7x_8x_9 \oplus x_0x_8x_9 \oplus x_0x_9 \oplus x_1x_2 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_4x_5x_6 \oplus$
 $x_1x_2x_3x_4x_5x_6x_7x_8 \oplus x_1x_2x_3x_4x_5x_6x_7x_9 \oplus x_1x_2x_3x_4x_5x_6x_8 \oplus x_1x_2x_3x_4x_5x_6x_8x_9 \oplus x_1x_2x_3x_4x_5x_7 \oplus x_1x_2x_3x_4x_5x_7x_8x_9 \oplus$
 $x_1x_2x_3x_4x_5x_7x_9 \oplus x_1x_2x_3x_4x_5x_8 \oplus x_1x_2x_3x_4x_5x_9 \oplus x_1x_2x_3x_4x_6 \oplus x_1x_2x_3x_4x_6x_7 \oplus x_1x_2x_3x_4x_6x_7x_8 \oplus x_1x_2x_3x_4x_6x_7x_8x_9 \oplus$
 $x_1x_2x_3x_4x_6x_8x_9 \oplus x_1x_2x_3x_4x_6x_9 \oplus x_1x_2x_3x_4x_7x_8 \oplus x_1x_2x_3x_4x_7x_9 \oplus x_1x_2x_3x_4x_8 \oplus x_1x_2x_3x_4x_8x_9 \oplus x_1x_2x_3x_5 \oplus$
 $x_1x_2x_3x_5x_6x_7 \oplus x_1x_2x_3x_5x_6x_7x_8x_9 \oplus x_1x_2x_3x_5x_6x_7x_9 \oplus x_1x_2x_3x_5x_6x_8 \oplus x_1x_2x_3x_5x_6x_9 \oplus x_1x_2x_3x_5x_7 \oplus$
 $x_1x_2x_3x_5x_7x_8 \oplus x_1x_2x_3x_5x_7x_8x_9 \oplus x_1x_2x_3x_5x_8x_9 \oplus x_1x_2x_3x_5x_9 \oplus x_1x_2x_3x_6 \oplus x_1x_2x_3x_6x_7x_8 \oplus x_1x_2x_3x_6x_7x_9 \oplus$
 $x_1x_2x_3x_6x_8 \oplus x_1x_2x_3x_6x_8x_9 \oplus x_1x_2x_3x_7 \oplus x_1x_2x_3x_7x_8x_9 \oplus x_1x_2x_3x_7x_9 \oplus x_1x_2x_3x_8 \oplus x_1x_2x_3x_9 \oplus x_1x_2x_4 \oplus$
 $x_1x_2x_4x_5 \oplus x_1x_2x_4x_5x_6 \oplus x_1x_2x_4x_5x_6x_7 \oplus x_1x_2x_4x_5x_6x_7x_8 \oplus x_1x_2x_4x_5x_6x_7x_8x_9 \oplus x_1x_2x_4x_5x_6x_8x_9 \oplus x_1x_2x_4x_5x_6x_9 \oplus$
 $x_1x_2x_4x_5x_7x_8 \oplus x_1x_2x_4x_5x_7x_9 \oplus x_1x_2x_4x_5x_8 \oplus x_1x_2x_4x_5x_8x_9 \oplus x_1x_2x_4x_6x_7 \oplus x_1x_2x_4x_6x_7x_8x_9 \oplus x_1x_2x_4x_6x_7x_9 \oplus$
 $x_1x_2x_4x_6x_8 \oplus x_1x_2x_4x_6x_9 \oplus x_1x_2x_4x_7 \oplus x_1x_2x_4x_7x_8 \oplus x_1x_2x_4x_7x_8x_9 \oplus x_1x_2x_4x_8x_9 \oplus x_1x_2x_4x_9 \oplus x_1x_2x_5x_6 \oplus$
 $x_1x_2x_5x_6x_7x_8 \oplus x_1x_2x_5x_6x_7x_9 \oplus x_1x_2x_5x_6x_8 \oplus x_1x_2x_5x_6x_8x_9 \oplus x_1x_2x_5x_7 \oplus x_1x_2x_5x_7x_8x_9 \oplus x_1x_2x_5x_7x_9 \oplus$
 $x_1x_2x_5x_8 \oplus x_1x_2x_5x_9 \oplus x_1x_2x_6 \oplus x_1x_2x_6x_7 \oplus x_1x_2x_6x_7x_8 \oplus x_1x_2x_6x_7x_8x_9 \oplus x_1x_2x_6x_8x_9 \oplus x_1x_2x_6x_9 \oplus x_1x_2x_7x_8 \oplus$
 $x_1x_2x_7x_9 \oplus x_1x_2x_8 \oplus x_1x_2x_8x_9 \oplus x_1x_3 \oplus x_1x_3x_4x_5 \oplus x_1x_3x_4x_5x_6x_7 \oplus x_1x_3x_4x_5x_6x_7x_8x_9 \oplus x_1x_3x_4x_5x_6x_7x_9 \oplus$
 $x_1x_3x_4x_5x_6x_8 \oplus x_1x_3x_4x_5x_6x_9 \oplus x_1x_3x_4x_5x_7 \oplus x_1x_3x_4x_5x_7x_8 \oplus x_1x_3x_4x_5x_7x_8x_9 \oplus x_1x_3x_4x_5x_8x_9 \oplus x_1x_3x_4x_5x_9 \oplus$
 $x_1x_3x_4x_6 \oplus x_1x_3x_4x_6x_7x_8 \oplus x_1x_3x_4x_6x_7x_9 \oplus x_1x_3x_4x_6x_8 \oplus x_1x_3x_4x_6x_8x_9 \oplus x_1x_3x_4x_7 \oplus x_1x_3x_4x_7x_8x_9 \oplus$
 $x_1x_3x_4x_7x_9 \oplus x_1x_3x_4x_8 \oplus x_1x_3x_4x_9 \oplus x_1x_3x_5 \oplus x_1x_3x_5x_6 \oplus x_1x_3x_5x_6x_7 \oplus x_1x_3x_5x_6x_7x_8 \oplus x_1x_3x_5x_6x_7x_8x_9 \oplus$
 $x_1x_3x_5x_6x_8x_9 \oplus x_1x_3x_5x_6x_9 \oplus x_1x_3x_5x_7x_8 \oplus x_1x_3x_5x_7x_9 \oplus x_1x_3x_5x_8 \oplus x_1x_3x_5x_8x_9 \oplus x_1x_3x_6x_7 \oplus x_1x_3x_6x_7x_8x_9 \oplus$
 $x_1x_3x_6x_7x_9 \oplus x_1x_3x_6x_8 \oplus x_1x_3x_6x_9 \oplus x_1x_3x_7 \oplus x_1x_3x_7x_8 \oplus x_1x_3x_7x_8x_9 \oplus x_1x_3x_8x_9 \oplus x_1x_3x_9 \oplus x_1x_4 \oplus$
 $x_1x_4x_5x_6 \oplus x_1x_4x_5x_6x_7x_8 \oplus x_1x_4x_5x_6x_7x_9 \oplus x_1x_4x_5x_6x_8 \oplus x_1x_4x_5x_6x_8x_9 \oplus x_1x_4x_5x_7 \oplus x_1x_4x_5x_7x_8x_9 \oplus$
 $x_1x_4x_5x_7x_9 \oplus x_1x_4x_5x_8 \oplus x_1x_4x_5x_9 \oplus x_1x_4x_6 \oplus x_1x_4x_6x_7 \oplus x_1x_4x_6x_7x_8 \oplus x_1x_4x_6x_7x_8x_9 \oplus x_1x_4x_6x_8x_9 \oplus$
 $x_1x_4x_6x_9 \oplus x_1x_4x_7x_8 \oplus x_1x_4x_7x_9 \oplus x_1x_4x_8 \oplus x_1x_4x_8x_9 \oplus x_1x_5 \oplus x_1x_5x_6x_7 \oplus x_1x_5x_6x_7x_8x_9 \oplus x_1x_5x_6x_7x_9 \oplus$
 $x_1x_5x_6x_8 \oplus x_1x_5x_6x_9 \oplus x_1x_5x_7 \oplus x_1x_5x_7x_8 \oplus x_1x_5x_7x_8x_9 \oplus x_1x_5x_8x_9 \oplus x_1x_5x_9 \oplus x_1x_6 \oplus x_1x_6x_7x_8 \oplus x_1x_6x_7x_9 \oplus$
 $x_1x_6x_8 \oplus x_1x_6x_8x_9 \oplus x_1x_7 \oplus x_1x_7x_8x_9 \oplus x_1x_7x_9 \oplus x_1x_8 \oplus x_1x_9 \oplus x_2 \oplus x_2x_3 \oplus x_2x_3x_4 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_4x_5x_6 \oplus$
 $x_2x_3x_4x_5x_6x_7 \oplus x_2x_3x_4x_5x_6x_7x_8 \oplus x_2x_3x_4x_5x_6x_7x_8x_9 \oplus x_2x_3x_4x_5x_6x_8x_9 \oplus x_2x_3x_4x_5x_6x_9 \oplus x_2x_3x_4x_5x_7x_8 \oplus$

$$\begin{aligned}
& 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
\end{aligned}$$

637 **Author Contributions.**

638 **Competing Interests.**

639 **Materials & Correspondence.**

640 References

- 641 [1] Yakir Aharonov and Lev Vaidman. “The Two-State Vector Formalism: An Updated Review”. In: *Time*
642 *in Quantum Mechanics*. Ed. by J.G. Muga, R. Sala Mayato, and Í.L. Egusquiza. Berlin, Heidelberg:
643 Springer Berlin Heidelberg, 2008, pp. 399–447.
- 644 [2] Stephen M. Barnett, John Jeffers, and David T. Pegg. “Quantum Retrodiction: Foundations and
645 Controversies”. In: *Symmetry* 13.4 (2021).
- 646 [3] Natalia Tokareva. “Chapter 1 - Boolean Functions”. In: *Bent Functions*. Ed. by Natalia Tokareva.
647 Boston: Academic Press, 2015, pp. 1–15.
- 648 [4] Satoshi Watanabe. “Symmetry of Physical Laws. Part III. Prediction and Retrodiction”. In: *Rev. Mod.*
649 *Phys.* 27 (2 Apr. 1955), pp. 179–186.