Optimal Self-Dual Inequalities to Order Polarized BECs

Ting-Chun Lin
University of California San Diego, CA, USA
Hai (Foxconn) Research Institute, Taipei, Taiwan
til022@ucsd.edu

Hsin-Po Wang
University of California, Berkeley, CA, USA
simple@berkeley.edu

***Abstract*— $1-(1-x^M)^{2^M} > (1-(1-x)^M)^{2^M}$ is proved for all $x \in [0,1]$ and all $M > 1$. This confirms a conjecture about polar code, made by Wu and Siegel in 2019, that $W^{0^m1^M}$ is more reliable than $W^{1^m0^M}$, where W is any binary erasure channel and $M = 2^m$. The proof relies on a remarkable relaxation that m needs not be an integer, a cleverly crafted hexavariate ordinary differential equation, and a genius generalization of Green's theorem that concerns function composition. The resulting inequality is optimal, M cannot be 2^m-1, witnessing how far polar code deviates from Reed–Muller code.**

I. Introduction

If there is anything that contributes to polar code's outstandingly low decoding complexity, it is the insistence of the successive cancellation decoder that some information bits are processed earlier and some later [1]. This, generally speaking, makes bits that are processed later better protected. For instance, if $abc1xyz$ is the binary expansion of a bit's index, it has been shown that it is better protected than the bit whose index's binary expansion reads $abc0xyz$. With a more elaborated argument, it was shown that $abc10xyz$ is better protected than $abc01xyz$ [2], [3].

It is very difficult to prove otherwise, that there exists an information bit that is processed earlier yet better protected. We do not know, for instance, whether the bit indexed by $abc011xyz$ is *always* better protected than the bit indexed by $abc100xyz$, despite of countless simulations that support so (to an extent that some works advocate postponing 011 and processing 100 first [4]–[6]). In this work, we give several examples over binary erasure channels (BEC) where a bit whose binary index is lexicographically earlier is always better protected. Some examples are 011 versus 100, 00111 versus 10000, 01011 versus 10100, 001111 versus 110000, 000111 versus 100000, and the list goes on.

For any BEC W with capacity $I(W) = x$, let W^0 be the BEC with capacity $I(W^0) = x^2$; let W^1 be the BEC with capacity $I(W^1) = 1-(1-x)^2$. For any binary string $b_1b_2\dots b_n \in \{0,1\}^n$, define $W^{b_1b_2\cdots b_n}$ as $\big(\cdots(W^{b_1})^{b_2}\cdots\big)^{b_n}$. For any binary strings $a \in \{0,1\}^m$ and $b \in \{0,1\}^n$, we say that the former outperforms the latter if, for any underlying BEC W, the capacity of W^a is higher than or equal to the capacity of W^b. We denote this as $a \succcurlyeq b$. When there are consecutive bits in a binary string, for instance 000 and , we abbreviate it as 0^3 and 1^5.

The main results of this work follows. We show that, to prove a comparison of the form $0^m1^n \succcurlyeq 1^m0^n$, it suffices to check if the comparison holds for $x = 1/2$.

Theorem 1 (main theorem): Let m and n be positive numbers. We have $0^m1^n \succcurlyeq 1^m0^n$ if and only if we have $(1-1/2^{2^m})^{2^n} \le 1/2$.

Theorem 1 resolves a conjecture by Wu and Siegel, which states that $0^m1^{2^m} \succcurlyeq 1^m0^{2^m}$ [7, (45)], as $(1-1/2^{2^m})^{2^{2^m}}$ is indeed $\le 1/2$. In fact, Theorem 1 implies something stronger: that $0^m1^{2^m-0.528} \succcurlyeq 1^m0^{2^m-0.528}$ for all $m > 0$. We hope that readers are not turned away by the unexpected notion that there are $2^m-0.528$ ones on the left-hand side and $2^m-0.528$ zeros on the right-hand side. We never said m, n are integers. Making sense of non-integer amounts of zeros and ones is the breakthrough that enables the proof of the main theorem.

This paper is organized as follows. Section II defines what 0^p and 1^q mean for real numbers p and q. Section III demonstrates the key idea of the main theorem using an example—we will prove that $1^p0^q \succcurlyeq 0^p1^q$ for any real numbers $p, q > 0$. Section IV discusses $0^p1^q \succcurlyeq 1^r0^s$ for small p, q, r, s. Section V generalizes Green's theorem to discuss the case when p, q, r, s are not small. Section VI proves the main theorem and some consequences.

II. Interpolating the Action of Squaring

In this section, we parametrize the action of squaring a number so it makes sense to say "I am 61.8% done with squaring this number."

For any real numbers p and q, define $I_0^p(x) \coloneqq x^{2^p}$ and $I_1^q(x) \coloneqq 1-(1-x)^{2^q}$. Note that $I_0^0(x)$ is just x, that $I_0^1(x)$ is just x^2, and that $I_0^r(I_0^p(x))$ is just $I_0^{p+r}(x)$. Consider real numbers $p_1, p_2, \dots, p_n$ and $q_1, q_2, \dots, q_n$. Let a *realistic string* be of the form $0^{p_1}1^{q_1}0^{p_2}1^{q_2}\cdots0^{p_n}1^{q_n}$ and correspond to the function composition

$$I_1^{q_n}\Big(I_0^{p_n}\Big(\cdots I_1^{q_2}\big(I_0^{p_2}\big(I_1^{q_1}\big(I_0^{p_1}(x)\big)\big)\big)\cdots\Big)\Big) \tag{1}$$

We say $0^{p_1}1^{q_1}0^{p_2}1^{q_2}\cdots0^{p_n}1^{q_n} \succcurlyeq 0^{r_1}1^{s_1}0^{r_2}1^{s_2}\cdots0^{r_n}1^{s_n}$ if formula (1) is greater than or equal to

$$I_1^{s_n}\Big(I_0^{r_n}\Big(\cdots I_1^{s_2}\big(I_0^{r_2}\big(I_1^{s_1}\big(I_0^{r_1}(x)\big)\big)\big)\cdots\Big)\Big)$$

for all $x \in [0,1]$.

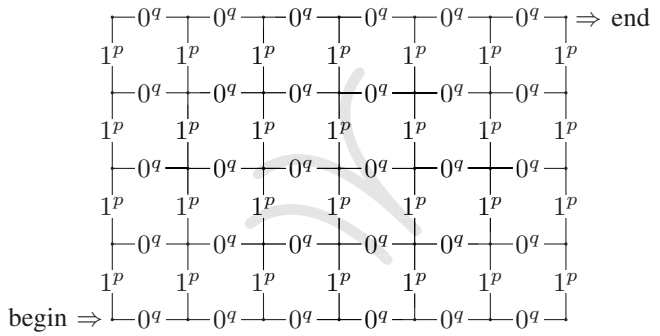

Fig. 1. Green's theorem and inequality: Suppose that every small square is such that going up-and-then-right results in a better reward than going right-and-then-up. Then the path that travels from the southwest corner to the northeast corner via the northwest corner yields better reward than that via the southeast corner. That is to says, $1^{4p}0^{6q} \succcurlyeq 0^{6q}1^{4p}$.

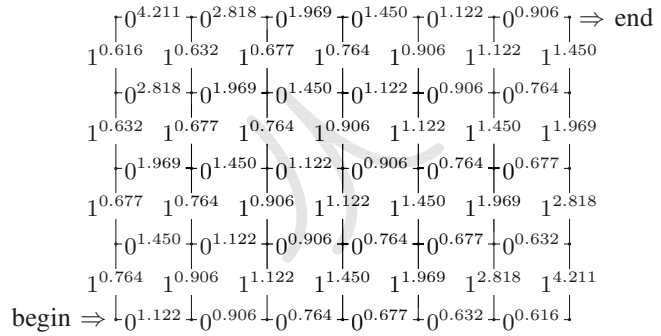

Fig. 2. Green's theorem and inequality: Similar to Figure 1 except that, here, the assumption is that going right-and-then-up is better. Thus the path via the southeast corner yields the highest reward among all paths. While numbers in this figure are found by a computer, we will prove mathematically that an ideal grid exists.

For all intents and purposes, we can safely ignore 0^0 and 1^0. We can also identify 0^p0^r as 0^{p+r} and 1^q1^s as 1^{q+s}. Through these simplifications, the notion of realistic string covers all possible concatenations of 0^p and 1^q.

Immediately one sees that $I_0^p(x) < x < I_1^q(x)$ for all $p, q > 0$ and $0 < x < 1$. Accordingly, one writes $0^p \preccurlyeq$ empty string $\preccurlyeq 1^q$. This is the continuous version of $0 \preccurlyeq$ empty string $\preccurlyeq 1$. The next section proves the continuous version of $01 \preccurlyeq 10$, illustrating our idea for the main theorem.

III. $1^p0^q \succcurlyeq 0^q1^p$: A Demonstration of Ideas

In this section, we want to show that for any pairs of positive real numbers (p, q) it holds that $1^p0^q \succcurlyeq 0^q1^p$. This serves as a toy example before we attack the main theorem.

To begin, we only care for very small p and q. That encourages us to consider the Taylor expansion of $I_0^q(I_1^p(x)) - I_1^p(I_0^q(x))$ at $(p, q) = (0, 0)$ while treating x as a constant. The expansion looks like

$$\begin{aligned} &I_0^q(I_1^p(x)) - I_1^p(I_0^q(x)) \\ &\quad = \ln(2)^2\Big(\ln(x)\ln(1-x) - x\ln(x) - (1-x)\ln(1-x)\Big)\cdot pq \\ &\qquad \pm O(|p|^3 + |q|^3). \end{aligned}$$

Clearly the term between the big parentheses is positive whenever $0 < x < 1$. Thus, for any $x \in [0, 1]$, the difference $I_0^q(I_1^p(x)) - I_1^p(I_0^q(x))$ is positive provided that p and q are positive yet small enough.

The punchline is that p and q need not be small.

Inspect Figure 1. In this figure, we want to travel from the southwest corner to the northeast corner. Each possible path corresponds to a realistic string. For instance, two rights, one up, four rights, and three ups means $0^{2q}1^p0^{4q}1^{3p}$. The inequality $1^p0^q \succcurlyeq 0^q1^p$ translates into a gimmick that, if a path lies northwest to another path, for instance $1^p0^{2q}1^{3p}0^{4q}$ is northwest to $0^{4q}1^{3p}0^{2q}1^p$, then the former $\succcurlyeq$ the latter, for instance $1^p0^{2q}1^{3p}0^{4q} \succcurlyeq 0^{4q}1^{3p}0^{2q}1^p$. Since Figure 1 can be made arbitrarily large with arbitrarily small squares, we conclude the following.

Theorem 2 (continuous version of $10 \succcurlyeq 01$*):* For any real numbers p and q that are positive, $1^p0^q \succcurlyeq 0^q1^p$. That is, $I_0^q(I_1^p(x)) \geq I_1^p(I_0^q(x))$ for all $0 \leq x \leq 1$.

The proof of the main theorem will follow the same logic. We first work out a local necessary condition for $I_1^q(I_0^p(x)) - I_0^s(I_1^r(x)) > 0$, and then we construct a big, fine grid on which we compare paths.

IV. Local Positivity for $0^p1^q \succcurlyeq 1^r0^s$

This section paves the way toward Theorem 1, the main theorem. More paving works will be done in the Section V, whereas the proof of the main theorem will be completed in Section VI. For the present section, our goal is to characterize the asymptotic behavior of the quadruples (p, q, r, s) such that $0^p1^q \succcurlyeq 1^r0^s$.

Applying Taylor approximation at the neighborhood of $(p, q, r, s) = (0, 0, 0, 0)$, we obtain

$$\begin{aligned} &I_1^q(I_0^p(x)) - I_0^s(I_1^r(x)) \\ &\quad = -\ln(2)x\ln(x)\cdot(s-p) \\ &\qquad -\ln(2)(1-x)\ln(1-x)\cdot(q-r) \\ &\qquad +\ln(2)^2x\ln(x)(1+\ln(1-x))\cdot pq \\ &\qquad +\ln(2)^2(1-x)\ln(1-x)(1+\ln x)\cdot rs \\ &\qquad \pm O(|p|^3 + |q|^3 + |r|^3 + |s|^3). \end{aligned}$$

To comprehend when the difference is nonnegative, we first want to understand when the Taylor approximation is barely nonnegative. That is to ask, what (p, q, r, s) makes $\Delta(y) = 0$ for some $y \in (0, 1)$ and $\Delta(x) > 0$ for any other $x \in (0, 1) \setminus y$, where

$$\begin{aligned} \Delta(x) \coloneqq &-\ln(2)x\ln(x)\cdot(s-p) \\ &-\ln(2)(1-x)\ln(1-x)\cdot(q-r) \\ &+\ln(2)^2x\ln(x)(1+\ln(1-x))\cdot pq \\ &+\ln(2)^2(1-x)\ln(1-x)(1+\ln x)\cdot rs? \end{aligned}$$

To proceed further, let us limit ourselves to the case where $s - p$ and $q - r$ are both of quadratic order. There is no

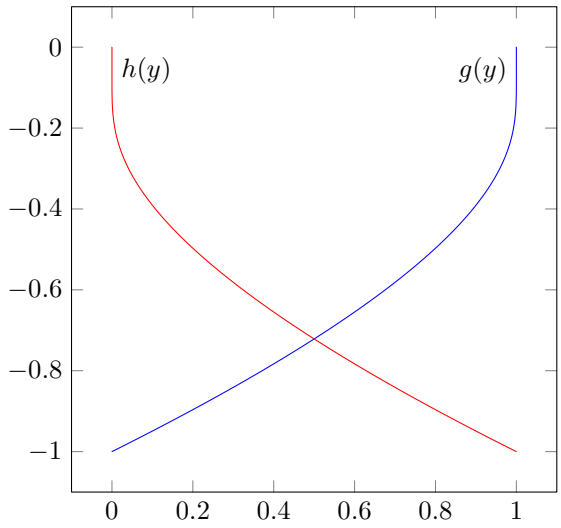

Fig. 3. Two of the coefficients in equation (2).

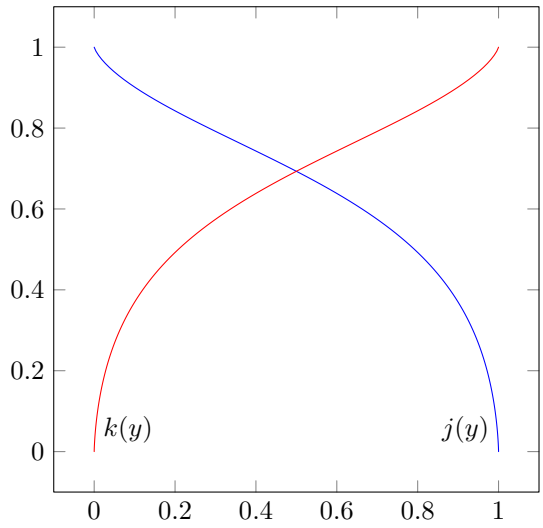

Fig. 4. The solution of equation (2) as functions in y.

rigorous justification why this should be the case. It just $feels\ right$, and it nevertheless leads to a rigorous proof of the main theorem. To elaborate, $s-p$ should be a polynomial in p, q, r, s without constant and linear term; similarly, $q-r$ should be a polynomial in p, q, r, s without constant and linear term; Henceforth,

$$rs = \big(p + O(\text{quadratic})\big)\big(q - O(\text{quadratic})\big) = pq + O(\text{cubic}).$$

We further limit ourselves to the case that $s-p$, $q-r$, pq, and rs are multiples of each other up to some cubic error. Again, we cannot explain why it must be like that; just bear with us.

Let j be $1-(s-p)/\ln(2)pq$. Let k be $1-(q-r)/\ln(2)pq$. This means that we can replace $s-p$ by $\ln(2)(1-j)pq$ and $q-r$ by $\ln(2)(1-k)pq$. The delta we want to make zero then simplifies to

$$\begin{aligned}\Delta(x) = {} & \ln(2)^2 \ln(x)\ln(1-x)\cdot pq \\ & + \ln(2)^2 x \ln(x) j \cdot pq \\ & + \ln(2)^2 (1-x)\ln(1-x) k \cdot pq.\end{aligned}$$

Factoring out $\ln(2)^2\ln(x)\ln(1-x)pq$, we conclude that the quadratic approximation is zero at $x = y$ if

$$1 + \frac{jy}{\ln(1-y)} + \frac{k(1-y)}{\ln y} = 0.$$

See Figure 3 for the plots of coefficients of j and k. See Figure 4 for the plots of j and k

Solving $\Delta(y) = 0$ for y is just the first half toward the characterization of (p, q, r, s) such that $\Delta(x) \geq 0$. The other equally important half is $\Delta'(y) = 0$. Together, we want to solve

$$\begin{bmatrix} g & h \\ g' & h' \end{bmatrix}\begin{bmatrix} j \\ k \end{bmatrix} = \begin{bmatrix} -1 \\ 0 \end{bmatrix}, \quad \text{where} \quad \begin{cases} g(y) := \frac{y}{\ln(1-y)}, \\ h(y) := \frac{1-y}{\ln y}. \end{cases} \tag{2}$$

Through this linear equation we encode the so-called *first-derivative test*. But the real question is whether $\Delta''(y) > 0$ or else it could be a local maximum. The answer is positive and is implied by the following four lemmas.

Lemma 3 (g'' and h''): $g(y)$ and $h(y)$ are strictly convex in y.

Lemma 4 (g' and h'): $g(y)$ is strictly monotonically increasing; $h(y)$ is strictly monotonically decreasing.

These two are clear from Figure 3, rigorous proofs found in appendices A and B.

Over the unit interval $(0, 1)$, the functions g and h form an *extended Chebyshev system* for the following reason: If we consider a linear combination $ag(y) + bh(y)$ where $ab > 0$, then the convexities of $g(y)$ and $h(y)$ imply that $ag(y)+bh(y)$ has at most two roots. If we consider $ag(y) + bh(y)$ where $ab < 0$, then it is either increasing or decreasing, guaranteeing a single root. In either case, $ag(y) + bh(y)$ has at most two roots. Hence the Wronskian (the determinant of the matrix in (2)) never collapses to zero.

We hereby conclude that for any $y \in (0, 1)$ there exist numbers j and k such that equation (2) is met. We view the solution (j, k) as functions in y.

Lemma 5 (j and k): $j(y)$ and $k(y)$ are positive whenever $0 < y < 1$.

Lemma 6 (j' and k'): $j(y)$ strictly monotonically decreases from 1 to 0 as y goes from 0 to 1. Meanwhile, $k(y)$ strictly monotonically increases from 0 to 1 as y goes from 0 to 1.

These properties are clear from Figure 4, rigorous proofs found in appendices C and D.

Proposition 7: For any $x, y \in (0, 1)$,

$$1 + \frac{j(y)x}{\ln(1-x)} + \frac{k(y)(1-x)}{\ln x} \geq 0.$$

The equality holds iff $x = y$.

Proof: Since j and k are positive and g and h are convex, $j(y)g(x)+k(y)h(x)$ will be convex in x. By the definitions of j and k, we know $j(y)g(x)+k(y)h(x)$ has both the evaluation and the first derivative zero at $x = y$. Therefore at $x = y$ is

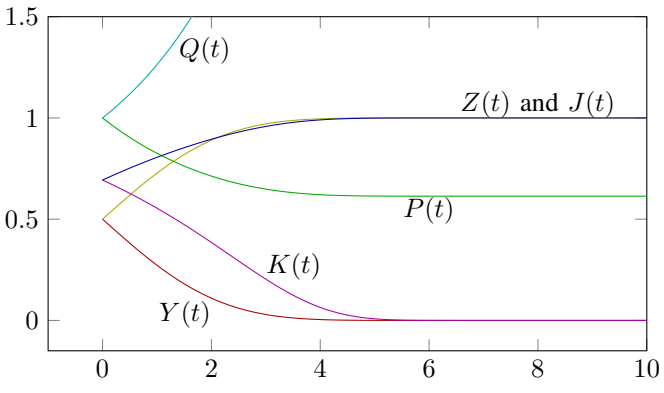

Fig. 5. The numerical solution of IVP 10. Horizontal axis is t.

a local minimum and for everywhere else, i.e., $x \neq y$, the evaluation is positive. ∎

Proposition 8: Fix any $x, y \in (0,1)$. Let p, q, r, s be such that $s-p = \ln(2)(1-j(y))pq$ and $q-r = \ln(2)(1-k(y))pq$. Then $\Delta(x) \geq 0$. The equality holds iff $x = y$.

Proof: Put the factor $\ln(2)^2 \ln(x) \ln(1-x)pq$ back. ∎

Here is a recap of what this section has so far. We inspect the Taylor expansion of $I_1^q(I_0^p(x)) - I_0^s(I_1^r(x))$ and extract a condition, equation (2), that we believe will lead to the positivity of Δ. Via analyzing the derivatives we do see that $\Delta(y) = 0$ granted that (2) is met; and if we plug-in any x other than y then $\Delta(x) > 0$. It is now time to apply these knowledge to construct a grid.

V. Green's Theorem for $0^p1^q \succcurlyeq 1^p0^q$

Local condition determined, we now want to construct a large, fine grid that looks like Figure 1, except that every small square represents a short inequality of the form $0^p1^q \succcurlyeq 1^r0^s$.

Figure 2 is a numerical example we found on a computer. In this figure, every small square, for instance the lower left one, corresponds to a local inequality of the form $0^{1.715}1^{1.259} \succcurlyeq 1^{1.015}0^{2.566}$. The ideal grid must satisfy two conditions. (A) The gap size must be infinitesimally small and the local condition must hold. That is, the delta as defined in the last section should be nonnegative but is zero at some point. (B) The value y such that $\Delta(y) = 0$ must aligns. Let us elaborate on (B).

Suppose there is an inequality $f(x) \geq g(x)$ and the equality holds for $x = 1/3$. Suppose there is $g(x) \geq h(x)$ and the equality holds for $x = 2/3$. Then $f(x) > g(x)$, but the equality never holds. In order to obtain the tightest inequality, i.e., the equality must hold at some point, it is inevitable that we aligns the points at which the sub-inequalities assume equality.

Since the point of equality changes continuously, it is best described by ordinary differential equations (ODEs). To solve ODE, we invoke the Picard–Lindelöf theorem.

Lemma 9 (Picard–Lindelöf): Let $n \in \mathbb{N}$. Let $I \subset \mathbb{R}$ be an open interval. Let $U \subset \mathbb{R}^n$ be an open rectangle. Let (t_0, y_0) be a point in $I \times U$. Suppose that a function $F\colon I \times U \to \mathbb{R}^n$ is continuous in the first argument and Lipschitz continuous in the second argument. Then the initial value problem

$$y(t_0) = y_0, \qquad \frac{d}{dt}y(t) = F(t, y(t))$$

has a unique solution for $t - t_0 \in [-\varepsilon, \varepsilon]$ for some very small $\varepsilon > 0$. (Proofs can be found on the internet.)

Using Lemma 9 one can prove that the following *initial value problem* (IVP) has a unique solution for sufficiently small t. Using some continuation techniques one can prove that the following IVP has na solution for all $t \in \mathbb{R}$.

Initial Value Problem 10: Let (Y, Z, P, Q, J, K) be real-valued functions in $t \in \mathbb{R}$ satisfying

$$\begin{aligned}
Y(0) &= \frac{1}{2}, & \frac{d}{dt}Y &= \ln(2)PY\ln Y,\\
Z(0) &= \frac{1}{2}, & \frac{d}{dt}Z &= -\ln(2)QZ\ln Z,\\
P(0) &= 1, & \frac{d}{dt}P &= -\ln(2)(1-J)PQ,\\
Q(0) &= 1, & \frac{d}{dt}Q &= \ln(2)(1-K)PQ,\\
J(0) &= \ln 2, & -1 &= \frac{Y}{\ln Z}\cdot J + \frac{Z}{\ln Y}\cdot K,\\
K(0) &= \ln 2, & 0 &= \frac{Z\ln Z + Y}{Z\ln(Z)^2}\cdot J - \frac{Y\ln Y + Z}{Y\ln(Y)^2}\cdot K.
\end{aligned}$$

Translation: t points to the southeast direction of the grid. Functions P and Q are the location-dependent version of p and q as in 0^p and 1^q. Functions J and K are the location-dependent version of j and k as in $s - p = \ln(2)(1-j)pq$ and $q - r = \ln(2)(1-k)pq$. Function Y will keep track of the y value in the context of equation (2). Function Z will be $1 - Y$. The last two equations are just (2).

Proposition 11: In IVP 10, $Y(t) + Z(t) = 1$ whenever defined.

Proof: $Y(t) + Z(t)$ satisfies a second-order ODE with initial values $Y(0)+Z(0) = 1$ and $Y'(0)+Z'(0) = 0$, thereby being constantly zero. ∎

Theorem 12: IVP 10 admits a unique solution for all $t \in \mathbb{R}$.

Proof: Thanks to symmetry it suffices to consider $t \geq 0$. Throughout the entire course of the dynamic system, the following bounds are maintained

$$\begin{aligned}
Y(t) &\in \left[2^{-2^t}, 1-2^{-2^{-t}}\right], & Z(t) &\in \left[2^{-2^{-t}}, 1-2^{-2^t}\right],\\
P(t) &\in \left[e^{1-2^t}, 1\right], & Q(t) &\in \left[1, 2^t\right],\\
J(t) &\in \left[k(2^{-2^{-t}}), j(2^{-2^t})\right], & K(t) &\in \left[k(2^{-2^t}), j(2^{-2^{-t}})\right].
\end{aligned}$$

Hence Picard–Lindelöf always applies. Every time Picard–Lindelöf is applied, the *domain of definition* (DoD) extends by a small but positive amount. By Zorn's lemma, the greatest DoD exists. If the greatest DoD is bounded, apply Picard–Lindelöf again to extend that DoD and get a contradiction. The greatest DoD, thereby, must cover the real line in its entirety. ∎

Forgive us for pausing here and appreciating how much trouble the preceding theorem has bypassed. When we applied the standard Runge–Kutta method to IVP 10, the solution

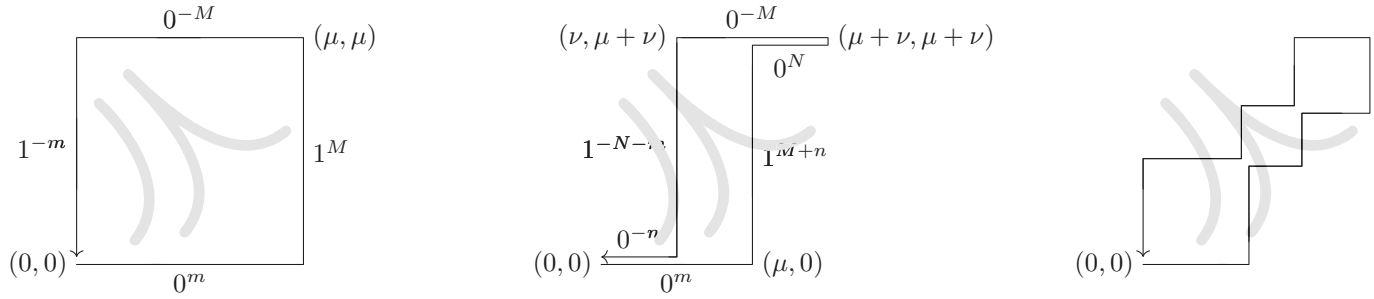

Fig. 6. Three loops that yield interesting results. Here, $m = \int_0^\mu P(t)\,dt = \int_{-\mu}^0 Q(t)\,dt$ and $M = \int_0^\mu Q(t)\,dt = \int_{-\mu}^0 P(t)\,dt$. Same for n, N, and ν.

explodes at about $t = 7.5$. This, as we perceive it, is because $Q(t)$ is about 1.4^t and so $Y(t)$ decays to zero doubly exponentially fast, which causes the machine to struggle with $\ln Z(t)$.

Definition 13 (path is the new string): Suppose $\Gamma(s) = (u(s), v(s)) \in \mathbb{R}^2$ is a piecewise smooth path parametrized by $s \in [0, S]$. Treat t as a function in s via $t(s) \coloneqq u(s) - v(s)$. Treat P and Q as functions in s via $P(t(s))$ and $Q(t(s))$. Consider this initial value problem of $X(s)$:

$$X(0) = x \in [0,1],$$
$$\frac{dX}{ds} = PX\ln(X)\cdot\frac{du}{ds} - (1-X)Q\ln(1-X)\cdot\frac{dv}{ds}.$$

Define $I_\Gamma(x)$ to be $X(S)$.

In plain text, the function X is defined as follows. Suppose Γ is a path on the u–v plane. Suppose at any point $\Gamma(s) \in \mathbb{R}^2$ on the path there associates a value $X(s) \in (0,1)$. The values are such that, every time Γ goes rightward by a tiny amount du, the associated value $X(s)$ evolves as $X(s+ds) = I_0^{du}(X(s))$. And every time Γ goes upward by a tiny amount dv, the associated value $X(s)$ evolves as $X(s+ds) = I_1^{dv}(X(s))$. Let I_Γ be the function composition of the infinitesimal I's.

Proposition 14 (travel with Y): Let $\Gamma(s) = (u(s), v(s)) \in \mathbb{R}^2$ be a piecewise smooth path parametrized by $s \in [0, S]$. Let $t(s) \coloneqq u(s) - v(s)$. Then it holds that $I_\Gamma(Y(t(0))) = Y(t(S))$. In particular, if Γ is such that $t(0) = t(S) = 0$, then $I_\Gamma(1/2) = 1/2$.

Proof: $X(s)$ and $Y(t(s))$ satisfy the same ODE and share the same initial condition. ∎

Theorem 15 ("Green's theorem"): $\Gamma(s) = (u(s), v(s)) \in \mathbb{R}^2$ is a piecewise smooth path that returns back to where it starts, i.e., $\Gamma(0) = \Gamma(S)$, but does not self-intersect elsewhere. Then $I_\Gamma(x) \geq x$ (respectively, $I_\Gamma(x) \leq x$) if Γ goes counterclockwise (respectively, clockwise). Moreover, the equality holds if $x = Y(u(0) - v(0))$.

Proof: Imagine a grid that looks like Figure 2 but the gap size δ is so small that we can safely ignore the cubic error term. Put $0^{P(u-v)\delta}$ on the vertical edge centered at (u, v) and $1^{Q(u-v)\delta}$ on the horizontal edge centered at (u, v). Then, for any small square with south edge 0^p, east edge 1^q, west edge 1^r, north edge 0^s, we know $I_0^p(I_1^q(I_0^{-s}(I_1^{-r}(x)))) \geq 0$ (up to cubic error), and the equality holds if x equals the value of Y at that point. Now $I_\Gamma(x)$ is just the grand total of all $I_0^p(I_1^q(I_0^{-s}(I_1^{-r}(x))))$. So $I_\Gamma(x) \geq 0$ and the equality holds if x equals the value of Y at the starting point. ∎

VI. Proof of the Main Theorem (Theorem 1) and Three More Consequences

The main theorem states that, if m and n are positive real numbers, $0^m1^n \succcurlyeq 1^m0^n$ if and only if $(1-1/2^{2^m})^{2^n} \leq 1/2$. Below is the proof.

Proof: Consider the path on the left of Figure 6. Applying Green's theorem's generalization (Theorem 15) to this path yields inequalities of the form $0^m1^M0^{-M}1^{-m} \succcurlyeq$ empty string. Here, $m = \int_0^\mu P(t)\,dt$ and $M = \int_0^\mu Q(t)\,dt$. By Proposition 14, $(1-1/2^{2^m})^{2^M} = 1/2$. Thus, $(1-1/2^{2^m})^{2^n} \leq 1/2$ iff $n \geq M$ iff $0^m1^n0^{-n}1^{-m} \succcurlyeq$ empty string iff $0^m1^n \succcurlyeq 1^m0^n$. This finishes the proof of the main theorem, Theorem 1. ∎

In the remainder of this section, let us list three more consequences.

Corollary 16 (square): $0^m1^M \succcurlyeq 1^m0^M$ for any positive real number m and $M \coloneqq 2^m + \log_2(\ln 2)$. Note that $\log_2(\ln 2) \approx -0.528$.

Proof: $(1-1/2^{2^m})^{2^M} \leq \exp(-2^M/2^{2^m}) \leq 1/2$ ∎

Corollary 17 (lightning): Suppose $m > n > 0$ are real numbers. Let M be a function in m determined by the equation $(1-1/2^{2^m})^{2^M} = 1/2$. Let N be a function in n determined by the equation $(1-1/2^{2^n})^{2^N} = 1/2$. Then $0^m1^M1^n0^N \succcurlyeq 0^n1^N1^m0^M$, which implies $0^{m-n}1^{M+n} \succcurlyeq 1^{N+m}0^{M-N}$.

Proof: Use the path at the center of Figure 6. ∎

Corollary 18 (Dyck Path): Let $n > 1$ be an integer. Suppose $a_j \in \{0,1\}$ and $b_j = 1 - a_j$ for all $j \in [n]$. Then $a_1 \cdots a_n \succcurlyeq b_1 \cdots b_n$ if $I_{a_1 \cdots a_m}(1/2) \leq 1/2$ for any $m \in [n-1]$ and $I_{a_1 \cdots a_n}(1/2) \geq 1/2$.

Proof: Use a diagonally-symmetric path that looks like the right one in Figure 6. ∎

Mentioned in the introduction, $011 \succcurlyeq 100$ and $001111 \succcurlyeq 110000$ are consequences of Corollary 16; $00111 \succcurlyeq 10000$ and $000111 \succcurlyeq 100000$ are consequences of Corollary 17; and $01011 \succcurlyeq 10100$ is a consequence of Corollary 18.

VII. Conclusions

We confirms a conjecture that concerns how to compare bit channels in the construction of polar code. The technique is quite novel as we use the existence of solution, not the solution per se, of an IVP. Our results give quantitative

characterizations of how far away polar coder is from Reed–Muller code [8]–[12].

References

[1] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051–3073, July 2009.

[2] M. Bardet, V. Dragoi, A. Otmani, and J.-P. Tillich, "Algebraic properties of polar codes from a new polynomial formalism," in *2016 IEEE International Symposium on Information Theory (ISIT)*, July 2016, pp. 230–234.

[3] C. Schürch, "A partial order for the synthesized channels of a polar code," in *2016 IEEE International Symposium on Information Theory (ISIT)*, July 2016, pp. 220–224.

[4] S. Buzaglo, A. Fazeli, P. H. Siegel, V. Taranalli, and A. Vardy, "Permuted successive cancellation decoding for polar codes," in *2017 IEEE International Symposium on Information Theory (ISIT)*, June 2017, pp. 2618–2622.

[5] G. Trofimiuk and P. Trifonov, "Window processing of binary polarization kernelswindow processing of binary polarization kernels," *IEEE Transactions on Communications*, vol. 69, no. 7, pp. 4294–4305, July 2021.

[6] G. Li, M. Ye, and S. Hu, "Adjacent-bits-swapped polar codes: A new code construction to speed up polarization," in *2022 IEEE International Symposium on Information Theory (ISIT)*, 2022, pp. 2142–2147.

[7] W. Wu and P. H. Siegel, "Generalized partial orders for polar code bit-channels," *IEEE Transactions on Information Theory*, vol. 65, no. 11, pp. 7114–7130, Nov 2019.

[8] E. Arikan, "A performance comparison of polar codes and reed-muller codes," *IEEE Communications Letters*, vol. 12, no. 6, pp. 447–449, June 2008.

[9] ——, "A survey of reed-muller codes from polar coding perspective," in *2010 IEEE Information Theory Workshop on Information Theory (ITW 2010, Cairo)*, Jan 2010, pp. 1–5.

[10] M. Mondelli, S. H. Hassani, and R. L. Urbanke, "From polar to reed-muller codes: A technique to improve the finite-length performance," *IEEE Transactions on Communications*, vol. 62, no. 9, pp. 3084–3091, Sep. 2014.

[11] B. Li, H. Shen, and D. Tse, "A rm-polar codes," 2014. [Online]. Available: https://arxiv.org/abs/1407.5483

[12] E. Abbe and M. Ye, "Reed-muller codes polarize," *IEEE Transactions on Information Theory*, vol. 66, no. 12, pp. 7311–7332, Dec 2020.

Appendix A
Proof of Lemma 3

Lemma 3 states that $g''(y) > 0$ and $h''(y) > 0$.

Proof: Differentiate $y/\ln(1-y)$ twice, it remains to check whether $-\ln(1-y) \geq y/(1-y/2)$. Compute the Taylor series of both sides at $y = 0$ and compare coefficients. The left-hand side is $1/2, 1/3, 1/4, 1/5$, etc. The right-hand side is $1/2, 1/4, 1/8, 1/16$, etc. That will conclude the convexity of g. For the convexity of h, invoke $h(y) = g(1-y)$. ∎

Appendix B
Proof of Lemma 4

Lemma 4 states that $g'(y) > 0$ and $h'(y) < 0$.

Proof: As $y \to 0$ from the right, $g'(y) \to 1/2$ and is ever increasing. Hence g' is positive. For the positivity of h', invoke $h(y) = g(1-y)$. ∎

Appendix C
Proof of Lemma 5

Lemma 5 states that $j(y) > 0$ and $k(y) > 0$

Proof: Look at equation (2). In the second row of the matrix, the derivatives $g'(y)$ and $h'(y)$ are positive and negative, respectively. Hence j and k assumes the same sign. Now look at the first row; both $g(y)$ and $h(y)$ are negative. Hence j and k are both positive. ∎

Appendix D
Proof of Lemma 6

Lemma 6 states that $j'(y) < 0$ and $k'(y) > 0$ and that $j(0) = K(1) = 1$ and $j(1) = k(0) = 0$.

and $k(y) > 0$

Proof: Look at equation (2). Differentiating the first equation with respect to y, we get $gj' + hk' + h'j + h'k = 0$. Since $g'j + h'k = 0$, we infer that $gj' + hk' = 0$. As an aftereffect of g and h assuming the same sign (they are both negative), j' and k' assume opposite signs. Differentiating the second equation with respect to y, we get $g'j' + h'k' + g''j + h''k = 0$. As we know that $g''j + h''k > 0$ and $(g'j')(h'k') > 0$, it must be the case that $g'j'$ and $h'k'$ are both negative. This proves that j is strictly monotonically decreasing and k is strictly monotonically increasing. To finalize the proof, notice that $(j,k) = (1,0)$ at $y = 0$ and $(j,k) = (0,1)$ at $y = 1$. ∎

Appendix E
More Details of Proposition 11

It is clear that $(Y+Z)(0) = 1$ and $(Y+Z)'(0) = (\ln(2)PY\ln Y - \ln(2)QZ\ln Z)(0) = 0$ by the given initial values. It remains to find a relation between $(Y+Z)''$ and $(Y+Z)'$ and $(Y+Z)$. To begin,

$$\begin{aligned}
Y'' &= (\ln(2)PY\ln Y)' \\
&= \ln(2)P'Y\ln Y + \ln(2)(P\ln Y + P)Y' \\
&= \ln(2)^2(J-1)PQY\ln Y + \ln(2)(P\ln Y + P)Y', \\
Z'' &= -(\ln(2)QZ\ln Z)' \\
&= -\ln(2)Q'Z\ln Z - \ln(2)(Q\ln Z + Q)Z' \\
&= \ln(2)^2(K-1)PQZ\ln Z - \ln(2)(Q\ln Z + Q)Z'.
\end{aligned}$$

We are to add Y'' and Z'' together. The sum will contain a sub-formula $JY\ln Y + KZ\ln Z$, which can be replaced by $-\ln Y\ln Z$ thanks to the fifth equation in IVP 10. Afterward, we will replace Y' by $(Y+Z)' + \ln(2)QZ\ln Z$ and Z' by $(Y+Z)' - \ln(2)PY\ln Y$. Let us see what those steps lead us to.

$$\begin{aligned}
&(Y+Z)'' \\
&= \ln(2)^2PQ(JY\ln Y + KZ\ln Z - Y\ln Y - Z\ln Z) \\
&\quad + \ln(2)(P\ln Y + P)Y' - \ln(2)(Q\ln Z + Q)Z' \\
&= \ln(2)^2PQ(-\ln Y\ln Z - Y\ln Y - Z\ln Z) \\
&\quad + \ln(2)(P\ln Y + P)Y' - \ln(2)(Q\ln Z + Q)Z' \\
&= \ln(2)^2PQ(-\ln Y\ln Z - Y\ln Y - Z\ln Z) \\
&\quad + \ln(2)(P\ln Y + P - Q\ln Z - Q)(Y+Z)' \\
&\quad + \ln(2)^2(P\ln Y + P)QZ\ln Z \\
&\quad + \ln(2)^2(Q\ln Z + Q)PY\ln Y \\
&= \ln(2)^2PQ(Y+Z-1)\ln Y\ln Z \\
&\quad + \ln(2)(P\ln Y + P - Q\ln Z - Q)(Y+Z)'.
\end{aligned}$$

So $(Y+Z)$ does satisfy a second-order ODE.

APPENDIX F
MORE DETAILS OF THEOREM 12

With an assumption that $t \geq 0$, the claimed bounds

$$\begin{aligned} Y(t) &\in \left[2^{-2^t}, 1-2^{-2^{-t}}\right], & Z(t) &\in \left[2^{-2^{-t}}, 1-2^{-2^t}\right], \\ P(t) &\in \left[e^{1-2^t}, 1\right], & Q(t) &\in \left[1, 2^t\right], \\ J(t) &\in \left[k(2^{-2^{-t}}), j(2^{-2^t})\right], & K(t) &\in \left[k(2^{-2^t}), j(2^{-2^{-t}})\right] \end{aligned}$$

is obtained in the following order.

Lower bound on Q: The starting point is $Q(0) = 1$ and the derivative is positive, hence $Q(t) \geq 1$.

Upper bound on P: The starting point is $P(0) = 1$ and the derivative is negative, hence $P(t) \leq 1$.

Upper bound on Q: Note that $Q' \leq \ln(2)Q$. By Grönwall's inequality, $Q(t) \leq 2^t$.

Lower bound P: Note that $P' \geq -\ln(2)PQ \geq -\ln(2)2^t P$. By Grönwall's inequality, $P(t) \geq e^{1-2^t}$.

Lower bound on Y: Rewrite $Y' \geq \ln(2)Y \ln Y$ as $\ln(Y)' \geq \ln(2)\ln Y$. By Grönwall's inequality, $\ln Y \geq -\ln(2)2^t$. That is to say, $Y(t) \geq 2^{-2^t}$.

Lower bound on Z: Rewrite $Z' \geq -\ln(2)Z \ln Z$ as $\ln(Z)' \geq -\ln(2)\ln Z$. By Grönwall's inequality, $\ln Z \geq -\ln(2)2^{-t}$. That is to say, $Z(t) \geq 2^{-2^{-t}}$.

Upper bound on Z: This one is as simple as $Z(t) = 1 - Y(t) \leq 1 - 2^{-2^t}$.

Upper bound on Y: This one is as simple as $Y(t) = 1 - Z(t) \leq 1 - 2^{-2^{-t}}$.

Upper bound on J: Invoke $J(t) = j(Y(t)) \leq j(2^{-2^t})$.

Lower bound on K: Invoke $K(t) = k(Y(t)) \geq k(2^{-2^t})$

Lower bound on J: Invoke $J(t) = j(Y(t)) = k(Z(t)) \geq k(2^{-2^{-t}})$.

Upper bound on K: Invoke $K(t) = k(Y(t)) = j(Z(t)) \leq j(2^{-2^{-t}})$.