ON THE INDEPENDENCE NUMBER OF DE BRUIJN GRAPHS

PIETRO MAJER AND MATTEO NOVAGA

Abstract. We derive the asymptotic formula $\alpha(k,q) = \lambda_{k-1} q^k + o(q^k)$, where $\alpha(k,q)$ is the independence number of the de Bruijn graph $B(k,q)$, and λ_{k-1} is a constant arising from a variational problem on the unit $(k-1)$-dimensional cube. When $k=4$, we show the bounds $91/240 \le \lambda_3 \le 11/28$. For odd prime k, we analyse the binary case $q=2$ via a phase reduction on rotation orbits. For $k=11$ and $k=13$ this yields certified optimal constructions, which combined with a lifting theorem by Lichiardopol give exact formulas for $\alpha(11,q)$ and $\alpha(13,q)$ for all $q \ge 2$, extending the known cases $k = 3, 5, 7$.

Contents

1. Introduction

De Bruijn graphs are a classical object in combinatorics, graph theory, and information theory. Their origin goes back to de Bruijn's paper [5], while the Eulerian perspective was developed further by van Aardenne-Ehrenfest and de Bruijn in [2]. Standard references include Fredricksen's survey [8], the necklace construction of Fredricksen and Maiorana [7], Ralston's expository article [11], the survey chapter of Du, Cao, and Hsu on de Bruijn and Kautz digraphs [4], and the recent monograph of Etzion [6].

In this paper we study the independence number of de Bruijn graphs. This problem lies at the intersection of graph theory and coding theory: independent sets in de Bruijn graphs encode collections of words that avoid prescribed overlap patterns, and in several cases they are closely related to comma-free codes. Exact formulas are known only in a limited number of lengths, while the general asymptotic behaviour for fixed word length is governed by the variational constants introduced by Trotter and Winkler [12] and further analysed by the authors in [10].

For integers $k, q \ge 2$, we denote by $B(k,q)$ the de Bruijn digraph with vertex set $[q]^k$, where

$$[q] := \{0, 1, \dots, q-1\},$$

and with directed edges

$$x_1 x_2 \dots x_k \longrightarrow x_2 x_3 \dots x_k y, \qquad y \in [q].$$

Thus, for us the first parameter is the word length and the second is the alphabet size. We notice that other conventions can be found in the literature: for instance, the underlying simple graph is denoted $UB(q,k)$ in [9], while the same graph appears as $B(q,k)$ in [3].

2020 *Mathematics Subject Classification.* 05C35, 05C69, 68R10.

Key words and phrases. de Bruijn graph, independence number, comma-free codes, variational methods, computer-assisted proof.

We denote by $\alpha(k,q)$ the independence number of the *simple* graph obtained from $B(k,q)$ after deleting self-loops. Two vertices

$$u = x_1x_2\dots x_k, \qquad v = y_1y_2\dots y_k$$

are adjacent in the underlying graph if and only if one of the overlap relations

$$x_2x_3\dots x_k = y_1y_2\dots y_{k-1} \qquad \text{or} \qquad y_2y_3\dots y_k = x_1x_2\dots x_{k-1}$$

holds. The graph $B(k,q)$ has exactly q looped vertices, namely the constant words

$$0^k,\ 1^k,\ \dots,\ (q-1)^k.$$

When these self-loops are retained we write $\alpha_{\mathrm{loop}}(k,q)$ for the corresponding independence number. Since only the q constant vertices are affected, one has

$$\alpha_{\mathrm{loop}}(k,q) \le \alpha(k,q) \le \alpha_{\mathrm{loop}}(k,q) + q.$$

In particular, for fixed k the looped and loopless models have the same leading asymptotic coefficient as $q \to \infty$.

The independence problem for de Bruijn graphs has both a continuum asymptotic side and a finite, explicitly certifiable side, and the two viewpoints reinforce each other.

First, we show that for every fixed $k \ge 2$ the leading term of $\alpha(k,q)$, as $q \to \infty$, is given exactly by a variational constant λ_{k-1}. More precisely, as $q \to +\infty$ one has

$$\alpha(k,q) = \lambda_{k-1}q^k + o(q^k).$$

This identifies the asymptotic independence problem on de Bruijn graphs with the variational problem studied in [12, 10].

Second, we focus on the first unresolved case, namely $k = 4$. Here the aim is not an exact formula, but a sharper understanding of the extremal coefficient. We prove explicit bounds on λ_3, combining a soft upper bound from a seven-cycle inequality with a constructive lower bound obtained from an explicit base configuration and an inductive dyadic lift.

Third, we return to exact finite constructions in the binary prime cases $k = 11$ and $k = 13$. The phase reduction on rotation orbits shows that an extremal example is determined by one phase choice on each non-trivial orbit; the remaining task is finite and computer-verifiable. We record fully specified certificates and deduce exact formulas for the independence number for every alphabet size $q \ge 2$.

The case $k = 4$ sits between several lengths for which the independence number is already understood exactly.

Theorem 1 (see [9, 3])**.** *There holds*

$$\begin{aligned}
&\alpha(2,2) = 2, && \alpha_{\mathrm{loop}}(2,2) = 1,\\
&\alpha(2,3) = 3, && \alpha_{\mathrm{loop}}(2,3) = 2,\\
&\alpha(2,q) = \alpha_{\mathrm{loop}}(2,q) = \left\lfloor \frac{q^2}{4} \right\rfloor && \text{for every } q \ge 4,\\
&\alpha(3,q) = \frac{q^3-q}{3} + 1, && \alpha_{\mathrm{loop}}(3,q) = \frac{q^3-q}{3}.\\
&\alpha(5,q) = \frac{2(q^5-q)}{5} + 1, && \alpha_{\mathrm{loop}}(5,q) = \frac{2(q^5-q)}{5},\\
&\alpha(7,q) = \frac{3(q^7-q)}{7} + 1, && \alpha_{\mathrm{loop}}(7,q) = \frac{3(q^7-q)}{7}.
\end{aligned}$$

Moreover, if $k \ge 3$ is an odd prime, then for every $q \ge 2$ we have

$$\alpha(k,q) \le \frac{(k-1)(q^k-q)}{2k} + 1, \qquad \alpha_{\mathrm{loop}}(k,q) \le \frac{(k-1)(q^k-q)}{2k}.$$

In Theorems 27 and 29 below, we extend the previous result to the next prime cases $k = 11$ and $k = 13$, and prove that

$$\alpha(11,q) = \frac{5(q^{11}-q)}{11} + 1, \quad \alpha_{\mathrm{loop}}(11,q) = \frac{5(q^{11}-q)}{11},$$

and

$$\alpha(13,q)=\frac{6(q^{13}-q)}{13}+1,\quad \alpha_{\mathrm{loop}}(13,q)=\frac{6(q^{13}-q)}{13}.$$

By contrast, no exact formula is presently known for $\alpha(4,q)$. This makes the length 4 case the first genuinely open instance, and one of the main motivations of the present work is to determine explicit bounds for its leading asymptotic coefficient.

For every integer $m\geq 1$ and every measurable set $A\subseteq[0,1]^m$, we now define

$$\Phi_m(A):=\int_{[0,1]^{m+1}}\mathbf{1}_A(x_1,\dots,x_m)\big(1-\mathbf{1}_A(x_2,\dots,x_{m+1})\big)\,dx_1\cdots dx_{m+1},\tag{1}$$

and set

$$\lambda_m:=\sup\{\Phi_m(A):A\subseteq[0,1]^m\text{ measurable}\}.\tag{2}$$

These constants were first introduced in [12], with a different definition, and the variational characterization in (1) was later given in [10]. As stated above, these constants also govern the independence number of de Bruijn graphs for large q: for every fixed $k\geq 2$, the asymptotic coefficient of $\alpha(k,q)$ is exactly λ_{k-1}.

Trotter and Winkler showed in [12] the strict monotonicity of the sequence λ_m, and proved the bounds

$$\frac{m}{2m+2}\leq\lambda_m\leq\frac{m}{2m+1},$$

together with the identities $\lambda_1=1/4$, $\lambda_2=1/3$ and the inequality $\lambda_5\geq 27/64$. The authors of this paper showed in [10] that

$$\lambda_m=\frac{m}{2m+2}\qquad\text{for every even } m,$$

and therefore for every odd word length k one obtains the exact asymptotic coefficient

$$\frac{\alpha(k,q)}{q^k}\longrightarrow\lambda_{k-1}=\frac{k-1}{2k}.$$

Moreover, Proposition 8 below yields a refined upper bound for odd k, while preserving the explicit lower bound coming from the elementary construction:

$$\frac{k-1}{2k}q^k-O(q^{k-2})\leq\alpha(k,q)\leq\frac{k-1}{2k}q^k+O(q^{\delta(k)}),$$

where the parameter $\delta(k)$ is defined in Proposition 8: it equals 1 if k is prime and k/p if k is composite, with p the smallest prime divisor of k. In particular, for odd prime k the error term in the upper bound is of order $O(q)$, consistently with the exact formulas quoted above for $k=3,5,7,11,13$.

The even-length case is more delicate. Already for $k=4$, the general bounds imply only

$$\frac{3}{8}\leq\lambda_3<\frac{2}{5}.$$

Our second main result improves this interval to

$$\frac{91}{240}\leq\lambda_3\leq\frac{11}{28},$$

and consequently

$$\frac{91}{240}q^4+o(q^4)\leq\alpha(4,q)\leq\frac{11}{28}q^4+o(q^4).$$

Thus, although the exact value of λ_3 remains open, the admissible range becomes substantially narrower.

For the reader's convenience, we summarise the main contributions of the paper.

1) We prove that for every fixed $k\geq 2$ the independence number of the de Bruijn graph satisfies
$$\alpha(k,q)=\lambda_{k-1}q^k+o(q^k),$$
thereby identifying the exact asymptotic coefficient with the continuum variational constant λ_{k-1}.

2) In the case $k = 4$, we establish the explicit bounds
$$\frac{91}{240} \le \lambda_3 \le \frac{11}{28}.$$
The upper bound is obtained from a combinatorial inequality on a 7-cycle, while the lower bound comes from an inductive dyadic construction starting from an explicit finite configuration.
3) For binary words of prime length, we introduce a phase reduction on rotation orbits. Combined with certified constructions, this yields exact formulas for $\alpha(11, q)$ and $\alpha(13, q)$ for all $q \ge 2$.

The paper is organised as follows. In Section 2 we reformulate the discrete extremal problem in a way that makes the connection with the variational constants λ_m transparent, and we prove the asymptotic formula for every fixed k. Section 3 is devoted to the case $k = 4$: we first derive the upper bound for λ_3, then construct the dyadic lower bound, and finally translate these bounds into corresponding estimates for $\alpha(4, q)$. To keep the main argument readable, the large explicit $q = 16$ data defining the base configuration are recorded separately in Appendix A, where we record both the explicit data defining the base configuration and the finite verification attached to it. In Section 4 we recall the phase reduction for odd prime binary lengths and use it to record the certified cases $k = 11$ and $k = 13$. Appendix B records a certificate for each of the cases $k = 11$ and $k = 13$, together with a short verifier script.

Acknowledgements. The authors acknowledge support from the MIUR Excellence Department Project awarded to the Department of Mathematics, University of Pisa, CUP I57G22000700001. M.N. is a member of INDAM-GNAMPA.

2. The asymptotic coefficient

Fix integers $k \ge 2$ and $q \ge 1$. Independent sets in $B(k, q)$ are naturally encoded by subsets of $[q]^{k-1}$.

Definition 2. *For $S \subseteq [q]^{k-1}$, define*
$$\mathcal{I}_{k,q}(S) := \big\{(x_1, \dots, x_k) \in [q]^k : (x_1, \dots, x_{k-1}) \in S,\ (x_2, \dots, x_k) \notin S\big\}.$$
Equivalently, $\mathcal{I}_{k,q}(S)$ consists of the words of length k whose prefix of length $k-1$ belongs to S and whose suffix of length $k-1$ does not. We also set
$$N_{k,q}(S) := |\mathcal{I}_{k,q}(S)|.$$

Proposition 3. *Define*
$$M_{k,q} := \max\big\{N_{k,q}(S) : S \subseteq [q]^{k-1}\big\}.$$
Then
$$M_{k,q} = \alpha_{\mathrm{loop}}(k, q).$$
Moreover,
$$M_{k,q} \le \alpha(k, q) \le M_{k,q} + q,$$
so in particular
$$\alpha(k, q) = M_{k,q} + O(q) \qquad (k \text{ fixed},\ q \to \infty).$$

Proof. Fix $S \subseteq [q]^{k-1}$. $\mathcal{I}_{k,q}(S)$ is an independent set in the graph with loops retained. Let
$$x = (x_1, \dots, x_k) \in \mathcal{I}_{k,q}(S).$$
By definition,
$$(x_1, \dots, x_{k-1}) \in S, \qquad (x_2, \dots, x_k) \notin S.$$
Suppose that a successor
$$y = (x_2, \dots, x_k, t) \qquad (t \in [q])$$
also belonged to $\mathcal{I}_{k,q}(S)$. Then, by the defining condition for $\mathcal{I}_{k,q}(S)$, its prefix $(x_2, \dots, x_k)$ would have to lie in S, a contradiction. Thus x is adjacent to no successor in $\mathcal{I}_{k,q}(S)$. The same

argument applied to predecessors shows that no predecessor of x can belong to $\mathcal{I}_{k,q}(S)$ either. Hence no two vertices of $\mathcal{I}_{k,q}(S)$ are adjacent.

A looped constant vertex cannot occur in $\mathcal{I}_{k,q}(S)$, because a word a^k would require simultaneously $a^{k-1} \in S$ and $a^{k-1} \notin S$. Therefore $\mathcal{I}_{k,q}(S)$ is independent in the looped model, and so

$$\alpha_{\mathrm{loop}}(k,q) \geq |\mathcal{I}_{k,q}(S)| = N_{k,q}(S).$$

Taking the maximum over S yields

$$\alpha_{\mathrm{loop}}(k,q) \geq M_{k,q}.$$

Conversely, let J be an independent set in the graph with loops retained. Define

$$S_J := \big\{(x_1,\dots,x_{k-1}) \in [q]^{k-1} : \exists x_k \in [q] \text{ such that } (x_1,\dots,x_k) \in J\big\}.$$

If $(x_1,\dots,x_k) \in J$, then $(x_1,\dots,x_{k-1}) \in S_J$ by construction. We have $(x_2,\dots,x_k) \notin S_J$, for otherwise there would exist $t \in [q]$ such that $(x_2,\dots,x_k,t) \in J$, and these two vertices would be adjacent, contradicting the independence of J. Therefore every vertex of J belongs to $\mathcal{I}_{k,q}(S_J)$, hence

$$|J| \leq |\mathcal{I}_{k,q}(S_J)| = N_{k,q}(S_J) \leq M_{k,q}.$$

Taking the maximum over all looped independent sets J gives

$$\alpha_{\mathrm{loop}}(k,q) \leq M_{k,q}.$$

Combining the two inequalities proves the identity $M_{k,q} = \alpha_{\mathrm{loop}}(k,q)$.

Finally, passing from the looped graph to the simple graph only affects the q constant vertices a^k. Hence one may gain at most q additional vertices when the loops are deleted, and therefore

$$M_{k,q} = \alpha_{\mathrm{loop}}(k,q) \leq \alpha(k,q) \leq \alpha_{\mathrm{loop}}(k,q) + q = M_{k,q} + q.$$

□

Thus $M_{k,q}$ is the basic discrete quantity. Once its asymptotics are known, those of $\alpha(k,q)$ follow from the additive error term q.

For $\mathbf{u} = (u_1,\dots,u_{k-2}) \in [q]^{k-2}$, we define

$$I_S(\mathbf{u}) := \#\big\{a \in [q] : (a,u_1,\dots,u_{k-2}) \in S\big\},$$

$$O_S(\mathbf{u}) := \#\big\{b \in [q] : (u_1,\dots,u_{k-2},b) \in S\big\}.$$

When $k = 2$, the index set $[q]^0$ is understood as the singleton $\{\emptyset\}$, so $I_S(\emptyset) = O_S(\emptyset) = |S|$.

A direct counting argument gives

$$N_{k,q}(S) = \sum_{\mathbf{u} \in [q]^{k-2}} I_S(\mathbf{u})\big(q - O_S(\mathbf{u})\big). \tag{3}$$

Indeed, for each fixed middle block $\mathbf{u}$, a word counted by $N_{k,q}(S)$ is obtained by choosing a prefix letter a such that $(a,\mathbf{u}) \in S$ and a suffix letter b such that $(\mathbf{u},b) \notin S$.

For $S \subseteq [q]^{k-1}$ and $(a_1,\dots,a_{k-1}) \in [q]^{k-1}$ we let

$$Q^{(q)}_{a_1\dots a_{k-1}} := \prod_{j=1}^{k-1} \Big[\frac{a_j}{q}, \frac{a_j+1}{q}\Big) \subseteq [0,1]^{k-1},$$

and

$$A_S := \bigcup_{(a_1,\dots,a_{k-1}) \in S} Q^{(q)}_{a_1\dots a_{k-1}} \subseteq [0,1]^{k-1}.$$

Similarly, for $(a_1,\dots,a_k) \in [q]^k$ let

$$Q^{(q)}_{a_1\dots a_k} := \prod_{j=1}^{k} \Big[\frac{a_j}{q}, \frac{a_j+1}{q}\Big) \subseteq [0,1]^{k}.$$

Lemma 4. *For every $S \subseteq [q]^{k-1}$ one has*

$$\Phi_{k-1}(A_S) = \Lambda_{k,q}(S) := \frac{N_{k,q}(S)}{q^k}.$$

Proof. Partition $[0,1]^k$ into the q^k cubes $Q^{(q)}_{a_1\dots a_k}$. On such a cube the integrand in (1), with $m = k-1$, is constant and equals

$$\mathbf{1}_S(a_1,\dots,a_{k-1})\big(1-\mathbf{1}_S(a_2,\dots,a_k)\big).$$

Since each cube has volume q^{-k}, summing over all cubes gives

$$\Phi_{k-1}(A_S) = q^{-k}\sum_{(a_1,\dots,a_k)\in[q]^k} \mathbf{1}_S(a_1,\dots,a_{k-1})\big(1-\mathbf{1}_S(a_2,\dots,a_k)\big) = \frac{N_{k,q}(S)}{q^k}.$$

□

Lemma 5. *For all measurable sets $A, B \subseteq [0,1]^{k-1}$,*

$$|\Phi_{k-1}(A) - \Phi_{k-1}(B)| \le 2\,\|\mathbf{1}_A - \mathbf{1}_B\|_{L^1([0,1]^{k-1})} = 2|A\triangle B|.$$

Proof. Write

$$\begin{aligned}\Phi_{k-1}(A) - \Phi_{k-1}(B) = \int_{[0,1]^k} \Big(&\mathbf{1}_A(x_1,\dots,x_{k-1})(1-\mathbf{1}_A(x_2,\dots,x_k))\\ &- \mathbf{1}_B(x_1,\dots,x_{k-1})(1-\mathbf{1}_B(x_2,\dots,x_k))\Big)\,dx_1\cdots dx_k\\ = \int_{[0,1]^k} &\big(\mathbf{1}_A(x_1,\dots,x_{k-1}) - \mathbf{1}_B(x_1,\dots,x_{k-1})\big)\big(1-\mathbf{1}_A(x_2,\dots,x_k)\big)\,dx\\ &+ \int_{[0,1]^k} \mathbf{1}_B(x_1,\dots,x_{k-1})\big(\mathbf{1}_B(x_2,\dots,x_k) - \mathbf{1}_A(x_2,\dots,x_k)\big)\,dx.\end{aligned}$$

Taking absolute values and using $0 \le \mathbf{1}_A, \mathbf{1}_B \le 1$ gives

$$\begin{aligned}|\Phi_{k-1}(A) - \Phi_{k-1}(B)| \le &\int_{[0,1]^k} \big|\mathbf{1}_A(x_1,\dots,x_{k-1}) - \mathbf{1}_B(x_1,\dots,x_{k-1})\big|\,dx\\ &+ \int_{[0,1]^k} \big|\mathbf{1}_A(x_2,\dots,x_k) - \mathbf{1}_B(x_2,\dots,x_k)\big|\,dx.\end{aligned}$$

In each integral one variable is free over an interval of length 1, so both terms equal $\|\mathbf{1}_A - \mathbf{1}_B\|_{L^1([0,1]^{k-1})}$. This completes the proof. □

Lemma 6. *For every measurable set $A \subseteq [0,1]^{k-1}$ there exist sets $A_q \subseteq [0,1]^{k-1}$, each of them a union of q-adic cubes of the form $Q^{(q)}_{a_1\dots a_{k-1}}$, such that*

$$|A_q\triangle A| \longrightarrow 0 \qquad \text{as } q\to\infty.$$

Equivalently,

$$\mathbf{1}_{A_q} \to \mathbf{1}_A \qquad \text{in } L^1([0,1]^{k-1}).$$

Proof. Let $\mathcal{G}_q$ be the sigma-algebra generated by the partition of $[0,1]^{k-1}$ into the q^{k-1} cubes $Q^{(q)}_{a_1\dots a_{k-1}}$. Set

$$u_q := \mathbb{E}(\mathbf{1}_A \mid \mathcal{G}_q).$$

Then u_q is constant on each q-adic cube, satisfies $0 \le u_q \le 1$, and we claim that

$$u_q \to \mathbf{1}_A \qquad \text{in } L^1([0,1]^{k-1}).$$

To see this, fix $\varepsilon > 0$ and choose a continuous function $\psi \in C([0,1]^{k-1})$ such that

$$\|\mathbf{1}_A - \psi\|_{L^1} < \varepsilon.$$

Conditional expectation is an L^1-contraction, so

$$\begin{aligned}\|u_q - \mathbf{1}_A\|_{L^1} &\le \|u_q - \mathbb{E}(\psi \mid \mathcal{G}_q)\|_{L^1} + \|\mathbb{E}(\psi \mid \mathcal{G}_q) - \psi\|_{L^1} + \|\psi - \mathbf{1}_A\|_{L^1} \\ &\le 2\varepsilon + \|\mathbb{E}(\psi \mid \mathcal{G}_q) - \psi\|_{L^1}.\end{aligned}$$

Because ψ is uniformly continuous and the diameters of the q-adic cubes tend to 0, the last term tends to 0. Hence $u_q \to \mathbf{1}_A$ in L^1.

For $t \in [0,1]$, let

$$E_q(t) := \{u_q > t\}.$$

Each $E_q(t)$ is a union of q-adic cubes. Moreover, for every point $x \in [0,1]^{k-1}$,

$$\int_0^1 \left|\mathbf{1}_{E_q(t)}(x) - \mathbf{1}_A(x)\right| dt = |u_q(x) - \mathbf{1}_A(x)|.$$

Integrating over x and applying Fubini yields

$$\int_0^1 |E_q(t) \triangle A|\, dt = \|u_q - \mathbf{1}_A\|_{L^1}.$$

Therefore there exists $t_q \in [0,1]$ such that

$$|E_q(t_q) \triangle A| \le \|u_q - \mathbf{1}_A\|_{L^1}.$$

Setting $A_q := E_q(t_q)$ proves the claim. □

Theorem 7. *For every fixed $k \ge 2$,*

$$\lim_{q\to\infty} \frac{M_{k,q}}{q^k} = \lambda_{k-1}.$$

Consequently,

$$\alpha(k,q) = \lambda_{k-1} q^k + o(q^k).$$

The same asymptotic formula also holds for $\alpha_{\mathrm{loop}}(k,q)$.

Proof. Fix q and let $S \subseteq [q]^{k-1}$. By Lemma 4,

$$\Phi_{k-1}(A_S) = \frac{N_{k,q}(S)}{q^k}.$$

Since λ_{k-1} is the supremum of Φ_{k-1} over all measurable sets, this gives

$$\frac{M_{k,q}}{q^k} \le \lambda_{k-1} \qquad \text{for every } q,$$

and hence

$$\limsup_{q\to\infty} \frac{M_{k,q}}{q^k} \le \lambda_{k-1}.$$

Conversely, let $\varepsilon > 0$. Choose a measurable set $A \subseteq [0,1]^{k-1}$ such that

$$\Phi_{k-1}(A) > \lambda_{k-1} - \varepsilon.$$

By Lemma 6, there exist q-adic sets A_q such that $|A_q \triangle A| \to 0$. Lemma 5 then implies

$$\Phi_{k-1}(A_q) \to \Phi_{k-1}(A).$$

Each A_q is of the form A_{S_q} for some $S_q \subseteq [q]^{k-1}$, and therefore

$$\frac{M_{k,q}}{q^k} \ge \frac{N_{k,q}(S_q)}{q^k} = \Phi_{k-1}(A_q).$$

For all sufficiently large q,

$$\frac{M_{k,q}}{q^k} \ge \Phi_{k-1}(A_q) > \Phi_{k-1}(A) - \varepsilon > \lambda_{k-1} - 2\varepsilon.$$

Thus

$$\liminf_{q\to\infty} \frac{M_{k,q}}{q^k} \ge \lambda_{k-1} - 2\varepsilon.$$

Since $\varepsilon > 0$ is arbitrary, we conclude that

$$\liminf_{q\to\infty} \frac{M_{k,q}}{q^k} \geq \lambda_{k-1}.$$

Combining this with the limsup bound proves

$$\lim_{q\to\infty} \frac{M_{k,q}}{q^k} = \lambda_{k-1}.$$

Finally, Proposition 3 gives

$$0 \leq \alpha(k,q) - M_{k,q} \leq q,$$

so dividing by q^k and using $M_{k,q}/q^k \to \lambda_{k-1}$ yields

$$\frac{\alpha(k,q)}{q^k} \to \lambda_{k-1}.$$

This proves the stated asymptotic formula. □

Proposition 8. *Assume that k is odd and define*

$$\delta(k) := \begin{cases} 1, & \text{if } k \text{ is prime,} \\ \dfrac{k}{p}, & \text{if } k \text{ is composite, where } p \text{ is the smallest prime divisor of } k. \end{cases}$$

Equivalently, for composite k, the quantity $\delta(k)$ is the largest proper divisor of k.

For each divisor $s \mid k$, let

$$\eta_s(q) := \frac{1}{s} \sum_{d|s} \mu(d)\, q^{s/d},$$

the number of cyclic rotation orbits in $[q]^k$ of size s. Then

$$M_{k,q} \leq U_k(q) := \frac{1}{2} \sum_{s|k} (s-1)\eta_s(q),$$

and therefore

$$M_{k,q} \leq \frac{k-1}{2k} q^k + O(q^{\delta(k)}).$$

Moreover,

$$M_{k,q} \geq \frac{k-1}{2k} q^k - O(q^{k-2}).$$

Consequently,

$$\frac{k-1}{2k} q^k - O(q^{k-2}) \leq M_{k,q} \leq \frac{k-1}{2k} q^k + O(q^{\delta(k)}),$$

and, by Proposition 3,

$$\frac{k-1}{2k} q^k - O(q^{k-2}) \leq \alpha(k,q) \leq \frac{k-1}{2k} q^k + O(q^{\delta(k)}).$$

In particular, if k is odd prime, then

$$M_{k,q} \leq \frac{k-1}{2k}(q^k - q), \qquad \alpha(k,q) \leq \frac{k-1}{2k} q^k + O(q).$$

Proof. We first prove the upper bound for $M_{k,q} = \alpha_{\mathrm{loop}}(k,q)$.

Let $\sigma : [q]^k \to [q]^k$ be the cyclic shift

$$\sigma(x_1, \dots, x_k) := (x_2, \dots, x_k, x_1).$$

For $x \in [q]^k$, let

$$\mathcal{O}(x) := \{x, \sigma x, \dots, \sigma^{s-1} x\}, \qquad s := |\mathcal{O}(x)|.$$

Since $\sigma^k = \mathrm{id}$, every orbit size s divides k. The vertices in $\mathcal{O}(x)$ form a directed cycle of length s in $B(k,q)$; when $s = 1$ this is a loop, and when $s \geq 2$ it is the usual directed cycle

$$x \to \sigma x \to \cdots \to \sigma^{s-1} x \to x.$$

Because k is odd, every divisor $s \mid k$ is odd. Hence the independence number of the induced subgraph on an orbit of size s in the looped model is exactly

$$\left\lfloor \frac{s}{2} \right\rfloor = \frac{s-1}{2},$$

with the case $s = 1$ included.

Therefore every looped independent set $J \subseteq [q]^k$ satisfies

$$|J| \leq \sum_{s|k} \frac{s-1}{2} \eta_s(q) = U_k(q),$$

where $\eta_s(q)$ denotes the number of σ-orbits of size s. Taking the maximum over all looped independent sets gives

$$M_{k,q} \leq U_k(q).$$

It remains to identify $\eta_s(q)$. A σ-orbit of size s is the same thing as a word of length k whose minimal period is s, modulo cyclic rotation. Such a word is obtained by repeating k/s times a primitive word of length s. The number of primitive words of length s is

$$\sum_{d|s} \mu(d)\, q^{s/d},$$

and dividing by s gives

$$\eta_s(q) = \frac{1}{s} \sum_{d|s} \mu(d)\, q^{s/d}.$$

Now isolate the contribution of $s = k$:

$$U_k(q) = \frac{k-1}{2} \eta_k(q) + \frac{1}{2} \sum_{\substack{s|k \\ s<k}} (s-1)\eta_s(q).$$

Since

$$\eta_k(q) = \frac{1}{k} \sum_{d|k} \mu(d)\, q^{k/d} = \frac{1}{k} q^k + O(q^{\delta(k)}),$$

and every proper divisor $s < k$ satisfies $s \leq \delta(k)$, we obtain

$$U_k(q) = \frac{k-1}{2k} q^k + O(q^{\delta(k)}).$$

This proves

$$M_{k,q} \leq \frac{k-1}{2k} q^k + O(q^{\delta(k)}).$$

For the lower bound we use the same explicit family as before. Let

$$S^{\mathrm{ev}}_{k,q} \subseteq [q]^{k-1}$$

be the set of $(u_1, \ldots, u_{k-1})$ such that the first occurrence of the maximum value among $u_1, \ldots, u_{k-1}$ is in an even position. We claim that a word

$$x = (x_1, \ldots, x_k) \in [q]^k$$

belongs to $\mathcal{I}_{k,q}(S^{\mathrm{ev}}_{k,q})$ if and only if the first occurrence of the maximum value among $x_1, \ldots, x_k$ is in an even position $t \in \{2, 4, \ldots, k-1\}$.

Indeed, if the first global maximum occurs at such a position t, then in the prefix $(x_1, \ldots, x_{k-1})$ the first occurrence of the maximum is also at position t, whereas in the suffix $(x_2, \ldots, x_k)$ it occurs at position $t-1$; hence the prefix lies in $S^{\mathrm{ev}}_{k,q}$ and the suffix does not. Conversely, if $x \in \mathcal{I}_{k,q}(S^{\mathrm{ev}}_{k,q})$, then the first occurrence of the maximum in the prefix is even and in the suffix is odd, so the first global maximum cannot occur at position 1 or k and must therefore occur at an even position $t \in \{2, 4, \ldots, k-1\}$.

Fix such an even position t and let $M \in \{0, \ldots, q-1\}$ be the maximum value. Then the first $t-1$ coordinates may be chosen arbitrarily in $\{0, \ldots, M-1\}$, the coordinate x_t must equal M,

and the remaining $k-t$ coordinates may be chosen arbitrarily in $\{0,\dots,M\}$. Hence the number of such words is

$$M^{t-1}(M+1)^{k-t}.$$

Summing over all admissible t and M yields

$$N_{k,q}(S^{\mathrm{ev}}_{k,q}) = \sum_{\substack{2\le t\le k-1\\ t \text{ even}}} \sum_{M=0}^{q-1} M^{t-1}(M+1)^{k-t}.$$

Expanding each summand,

$$M^{t-1}(M+1)^{k-t} = M^{k-1} + (k-t)M^{k-2} + O(M^{k-3}),$$

where the implied constant depends only on k. Since there are $(k-1)/2$ admissible values of t, and

$$\sum_{\substack{2\le t\le k-1\\ t \text{ even}}} (k-t) = \sum_{j=1}^{(k-1)/2} (k-2j) = \frac{(k-1)^2}{4},$$

we get

$$N_{k,q}(S^{\mathrm{ev}}_{k,q}) = \frac{k-1}{2}\sum_{M=0}^{q-1} M^{k-1} + \frac{(k-1)^2}{4}\sum_{M=0}^{q-1} M^{k-2} + O(q^{k-2}).$$

By Faulhaber's formula,

$$\sum_{M=0}^{q-1} M^{k-1} = \frac{q^k}{k} - \frac{1}{2}q^{k-1} + O(q^{k-2}), \qquad \sum_{M=0}^{q-1} M^{k-2} = \frac{q^{k-1}}{k-1} - \frac{1}{2}q^{k-2} + O(q^{k-3}).$$

Substituting these expansions gives

$$N_{k,q}(S^{\mathrm{ev}}_{k,q}) = \frac{k-1}{2k}q^k + \left(-\frac{k-1}{4} + \frac{k-1}{4}\right)q^{k-1} + O(q^{k-2}) = \frac{k-1}{2k}q^k + O(q^{k-2}).$$

Therefore

$$M_{k,q} \ge N_{k,q}(S^{\mathrm{ev}}_{k,q}) = \frac{k-1}{2k}q^k - O(q^{k-2}).$$

Finally, Proposition 3 yields

$$M_{k,q} \le \alpha(k,q) \le M_{k,q} + q.$$

Since $\delta(k) \ge 1$, the upper bound for $M_{k,q}$ implies

$$\alpha(k,q) \le \frac{k-1}{2k}q^k + O(q^{\delta(k)}),$$

and the lower bound for $M_{k,q}$ gives

$$\alpha(k,q) \ge \frac{k-1}{2k}q^k - O(q^{k-2}).$$

This completes the proof. □

Remark 9. *For odd composite k, the upper error term improves from $O(q^{k-2})$ to*

$$O(q^{\delta(k)}) = O(q^{k/p}),$$

where p is the smallest prime divisor of k; in particular $k/p < k-2$. For odd prime k, the upper bound is already of order $O(q)$. Thus the remaining gap is entirely on the lower-bound side: the present construction $S^{\mathrm{ev}}_{k,q}$ still gives only an error term of order q^{k-2}.

3. Asymptotic bounds for $k = 4$

For the rest of this section we fix $k = 4$. Accordingly, for every integer $q \geq 1$ and every set $S \subseteq [q]^3$ we write

$$N_q(S) := N_{4,q}(S), \qquad \Lambda_q(S) := \Lambda_{4,q}(S), \qquad \Phi := \Phi_3.$$

Our goal is to prove explicit upper and lower bounds for λ_3, and hence for the asymptotic independence ratio of $B(4, q)$.

3.1. **Upper bound via a seven-cycle inequality.** The upper bound in this section is independent of the dyadic construction and works simultaneously in the discrete and continuum settings.

For a finite set $S \subseteq [q]^3$ write

$$\rho_q(S) := \frac{|S|}{q^3}.$$

Lemma 10. *For every binary 7-tuple $y = (y_i)_{i\in\mathbb{Z}/7\mathbb{Z}} \in \{0,1\}^{\mathbb{Z}/7\mathbb{Z}}$ one has*

$$\sum_{i\in\mathbb{Z}/7\mathbb{Z}} y_i\big(1 - y_{i+1}\big) \leq 1 + \sum_{i\in\mathbb{Z}/7\mathbb{Z}} y_i\big(1 - y_{i+3}\big).$$

Proof. Let

$$B := \{i \in \mathbb{Z}/7\mathbb{Z} : y_i = 1\}.$$

For $s \in \{1, 3\}$ define

$$R_s(B) := \#\{i \in B : i + s \notin B\}.$$

Then the stated inequality is exactly

$$R_1(B) \leq R_3(B) + 1.$$

For every $s \in \{1, 3\}$ we have $R_s(B) = R_s(B^c)$: indeed, for the permutation $i \mapsto i + s$ of $\mathbb{Z}/7\mathbb{Z}$, the number of transitions $1 \to 0$ equals the number of transitions $0 \to 1$. Hence we may replace B by its complement and assume

$$|B| \leq 3.$$

If $B = \varnothing$, then $R_1(B) = R_3(B) = 0$ and there is nothing to prove. Assume now that $B \neq \varnothing$. Since $i \mapsto i+3$ is a single 7-cycle, some element of B must exit B under the step $+3$, so $R_3(B) \geq 1$. Therefore the claim is immediate whenever $R_1(B) \leq 2$. It remains only to consider the case

$$R_1(B) = 3.$$

Because $|B| \leq 3$, this forces $|B| = 3$, and the three elements of B are pairwise nonadjacent in the usual cycle on $\mathbb{Z}/7\mathbb{Z}$.

Assume for contradiction that $R_3(B) = 1$. Along the cyclic order generated by repeated addition of 3, the indicator of B changes from 1 to 0 exactly once, so B must be a single contiguous block in that $+3$-cycle. Since $|B| = 3$, there exists $t \in \mathbb{Z}/7\mathbb{Z}$ such that

$$B = \{t, t + 3, t + 6\}.$$

But t and $t+6 = t-1$ are adjacent in the usual cycle, contradicting $R_1(B) = 3$. Hence $R_3(B) \geq 2$, and therefore

$$R_1(B) = 3 \leq 2 + 1 \leq R_3(B) + 1.$$

This completes the proof. □

Proposition 11. *For every integer $q \geq 1$ and every set $S \subseteq [q]^3$,*

$$\Lambda_q(S) \leq \rho_q(S)\big(1 - \rho_q(S)\big) + \frac{1}{7} \leq \frac{11}{28}.$$

Equivalently,

$$N_q(S) \leq \left(\frac{11}{28}\right) q^4.$$

Proof. For each $i \in \mathbb{Z}/7\mathbb{Z}$, define

$$C_i := \big\{x = (x_0, \dots, x_6) \in [q]^7 : (x_i, x_{i+1}, x_{i+2}) \in S\big\},$$

with indices read modulo 7. For a fixed $x \in [q]^7$, set

$$y_i := \mathbf{1}_{C_i}(x) \in \{0, 1\}.$$

Applying Lemma 10 to the binary 7-tuple $(y_i)_{i\in\mathbb{Z}/7\mathbb{Z}}$ gives

$$\sum_{i\in\mathbb{Z}/7\mathbb{Z}} y_i(1 - y_{i+1}) \le 1 + \sum_{i\in\mathbb{Z}/7\mathbb{Z}} y_i(1 - y_{i+3}).$$

Since this inequality holds pointwise for every $x \in [q]^7$, summing over all x yields

$$\sum_{i\in\mathbb{Z}/7\mathbb{Z}} |C_i \setminus C_{i+1}| \le q^7 + \sum_{i\in\mathbb{Z}/7\mathbb{Z}} |C_i \setminus C_{i+3}|. \tag{4}$$

We evaluate the two sides of (4). By cyclic symmetry, the cardinalities do not depend on i. For $C_i \setminus C_{i+1}$, the condition $x \in C_i \setminus C_{i+1}$ is equivalent to

$$(x_i, x_{i+1}, x_{i+2}) \in S, \qquad (x_{i+1}, x_{i+2}, x_{i+3}) \notin S,$$

while the remaining three coordinates are arbitrary. Therefore

$$|C_i \setminus C_{i+1}| = q^3 N_q(S) = q^7 \Lambda_q(S).$$

Hence the left-hand side of (4) is $7q^7\Lambda_q(S)$.

For $C_i \setminus C_{i+3}$, the condition $x \in C_i \setminus C_{i+3}$ is equivalent to

$$(x_i, x_{i+1}, x_{i+2}) \in S, \qquad (x_{i+3}, x_{i+4}, x_{i+5}) \notin S,$$

with x_{i+6} arbitrary. Here the two displayed constraints involve disjoint coordinate triples, namely (x_i, x_{i+1}, x_{i+2}) and $(x_{i+3}, x_{i+4}, x_{i+5})$, while x_{i+6} is free. Thus

$$|C_i \setminus C_{i+3}| = |S|\,(q^3 - |S|)\,q = \rho_q(S)\big(1 - \rho_q(S)\big)q^7.$$

Hence the right-hand side of (4) is

$$q^7 + 7\rho_q(S)\big(1 - \rho_q(S)\big)q^7.$$

Substituting into (4) and dividing by $7q^7$, we obtain

$$\Lambda_q(S) \le \rho_q(S)\big(1 - \rho_q(S)\big) + \frac{1}{7}.$$

Since $\rho_q(S)(1 - \rho_q(S)) \le 1/4$, it follows that

$$\Lambda_q(S) \le \frac{1}{4} + \frac{1}{7} = \frac{11}{28}.$$

Multiplying by q^4 gives the equivalent bound for $N_q(S)$. □

Corollary 12. *One has*

$$\lambda_3 \le \frac{11}{28}.$$

Proof. This is the measure-theoretic analogue of Proposition 11. Let $A \subseteq [0, 1]^3$ be measurable, and write $|A| := \mathcal{L}^3(A)$. For each $i \in \mathbb{Z}/7\mathbb{Z}$, define

$$C_i := \big\{x = (x_0, \dots, x_6) \in [0, 1]^7 : (x_i, x_{i+1}, x_{i+2}) \in A\big\},$$

with indices read modulo 7. For a fixed $x \in [0, 1]^7$, set

$$y_i := \mathbf{1}_{C_i}(x) \in \{0, 1\}.$$

Applying Lemma 10 to the binary 7-tuple $(y_i)_{i\in\mathbb{Z}/7\mathbb{Z}}$ gives

$$\sum_{i\in\mathbb{Z}/7\mathbb{Z}} y_i(1 - y_{i+1}) \le 1 + \sum_{i\in\mathbb{Z}/7\mathbb{Z}} y_i(1 - y_{i+3}).$$

Integrating over $[0,1]^7$ yields

$$\sum_{i\in\mathbb{Z}/7\mathbb{Z}} \mathcal{L}^7(C_i \setminus C_{i+1}) \le 1 + \sum_{i\in\mathbb{Z}/7\mathbb{Z}} \mathcal{L}^7(C_i \setminus C_{i+3}). \tag{5}$$

Again, by cyclic symmetry the measures do not depend on i. For $C_i \setminus C_{i+1}$,

$$\mathcal{L}^7(C_i \setminus C_{i+1}) = \int_{[0,1]^7} \mathbf{1}_A(x_i, x_{i+1}, x_{i+2})\big(1 - \mathbf{1}_A(x_{i+1}, x_{i+2}, x_{i+3})\big)\, dx.$$

The integrand depends only on the four coordinates $(x_i, x_{i+1}, x_{i+2}, x_{i+3})$; after integrating out the remaining three free variables and relabelling $(u, v, w, z) = (x_i, x_{i+1}, x_{i+2}, x_{i+3})$, we obtain

$$\mathcal{L}^7(C_i \setminus C_{i+1}) = \int_{[0,1]^4} \mathbf{1}_A(u, v, w)\big(1 - \mathbf{1}_A(v, w, z)\big)\, dudvdwdz = \Phi(A).$$

Hence the left-hand side of (5) is $7\Phi(A)$.

For $C_i \setminus C_{i+3}$,

$$\mathcal{L}^7(C_i \setminus C_{i+3}) = \int_{[0,1]^7} \mathbf{1}_A(x_i, x_{i+1}, x_{i+2})\big(1 - \mathbf{1}_A(x_{i+3}, x_{i+4}, x_{i+5})\big)\, dx.$$

The two factors depend on disjoint triples of coordinates, while x_{i+6} is free. By Fubini,

$$\mathcal{L}^7(C_i \setminus C_{i+3}) = \left(\int_{[0,1]^3} \mathbf{1}_A\right)\left(\int_{[0,1]^3} (1 - \mathbf{1}_A)\right) = |A|(1 - |A|).$$

Therefore the right-hand side of (5) is

$$1 + 7|A|(1 - |A|).$$

Substituting into (5), we find

$$\Phi(A) \le |A|(1 - |A|) + \frac{1}{7} \le \frac{1}{4} + \frac{1}{7} = \frac{11}{28}.$$

Taking the supremum over measurable $A \subseteq [0,1]^3$ proves the claim. □

3.2. **Lower bound via a seven-site gadget.** We now construct an explicit dyadic family of sets that yields the lower bound $\lambda_3 \ge 91/240$.

Given $S \subseteq [q]^3$, its *dyadic lift* $L_q(S) \subseteq [2q]^3$ is defined by

$$(r, s, t) \in L_q(S) \iff \big(\lfloor r/2 \rfloor, \lfloor s/2 \rfloor, \lfloor t/2 \rfloor\big) \in S.$$

Lemma 13. *For every $q \ge 1$ and every $S \subseteq [q]^3$,*

$$N_{2q}(L_q(S)) = 16\, N_q(S).$$

Proof. A quadruple $(\alpha, \beta, \gamma, \delta) \in [q]^4$ contributes to $N_q(S)$ if and only if

$$(\alpha, \beta, \gamma) \in S, \qquad (\beta, \gamma, \delta) \notin S.$$

A quadruple $(r, s, t, u) \in [2q]^4$ contributes to $N_{2q}(L_q(S))$ if and only if its floor image $(\lfloor r/2 \rfloor, \lfloor s/2 \rfloor, \lfloor t/2 \rfloor, \lfloor u/2 \rfloor)$ contributes to $N_q(S)$; membership and non-membership are preserved under the floor map by definition of the lift. Each contributing quadruple in $[q]^4$ has exactly $2^4 = 16$ lifts to $[2q]^4$. Hence

$$N_{2q}(L_q(S)) = 16\, N_q(S).$$

□

The next ingredient is a local seven-site modification that increases the count by exactly one while preserving the local hypothesis needed for iteration.

Let $a, b \in [q]$ with $a \neq b$. We say that $H_q(a, b; S)$ holds if

$$\begin{aligned}
&\text{(i) } (a,a,a) \in S, \quad (b,b,a) \in S, \quad (b,a,a) \notin S, \quad (b,b,b) \notin S,\\
&\text{(ii) } I_S(a,a) + O_S(a,a) = q,\\
&\text{(iii) } I_S(b,b) + O_S(b,b) = q,\\
&\text{(iv) } I_S(b,b) + O_S(b,a) = q-1,\\
&\text{(v) } I_S(b,a) + O_S(a,a) = q+1.
\end{aligned}$$

Assume now that $H_q(a, b; S)$ holds, and set $X := L_q(S) \subseteq [2q]^3$. We define seven distinguished sites in $[2q]^3$:

$$\begin{aligned}
\text{Additions:} \quad & P_1 = (2b, 2b, 2b+1), \quad P_2 = (2b+1, 2b, 2b+1), \quad P_3 = (2b+1, 2a+1, 2a),\\
\text{Removals:} \quad & M_1 = (2a+1, 2a, 2a), \quad M_2 = (2a+1, 2a, 2a+1),\\
& M_3 = (2b, 2b+1, 2a), \quad M_4 = (2b, 2b+1, 2a+1).
\end{aligned}$$

All seven sites are pairwise distinct because $a \neq b$. Moreover, the membership part of $H_q(a, b; S)$ implies that

- the microcell above (b, b, b) is absent from X, so $P_1, P_2 \notin X$;
- the microcell above (b, a, a) is absent from X, so $P_3 \notin X$;
- the microcell above (a, a, a) is present in X, so $M_1, M_2 \in X$;
- the microcell above (b, b, a) is present in X, so $M_3, M_4 \in X$.

Hence the operation is genuinely "add the three P_i and remove the four M_j":

$$T := \big(X \cup \{P_1, P_2, P_3\}\big) \setminus \{M_1, M_2, M_3, M_4\}.$$

Lemma 14. *Under the same hypotheses,*

$$N_{2q}(T) = 16\, N_q(S) + 1.$$

Proof. By Lemma 13,

$$N_{2q}(X) = 16 N_q(S).$$

We compute the increment

$$\Delta N := N_{2q}(T) - N_{2q}(X)$$

using the degree formula (3). For $(u, v) \in [2q]^2$, set

$$\Delta I(u,v) := I_T(u,v) - I_X(u,v), \qquad \Delta O(u,v) := O_T(u,v) - O_X(u,v).$$

Expanding

$$(I_X + \Delta I)\big(2q - (O_X + \Delta O)\big) - I_X(2q - O_X)$$

inside the sum (3) gives

$$\Delta N = \sum_{u,v} \Big[\Delta I(u,v)\big(2q - O_X(u,v)\big) - I_X(u,v)\Delta O(u,v) - \Delta I(u,v)\Delta O(u,v)\Big].$$

Only finitely many ordered pairs (u, v) are affected. For each such pair we also record its coarse image $(\lfloor u/2 \rfloor, \lfloor v/2 \rfloor)$. Since $X = L_q(S)$, we have

$$I_X(u,v) = 2I_S(\lfloor u/2 \rfloor, \lfloor v/2 \rfloor), \qquad O_X(u,v) = 2O_S(\lfloor u/2 \rfloor, \lfloor v/2 \rfloor).$$

We first localise the effect of the seven toggled triples on the ordered pairs (u, v), and then rewrite the increment ΔN through a small collection of scalar balance quantities. A direct inspection

yields the following variation table:

(u,v)	$(\lfloor u/2\rfloor, \lfloor v/2\rfloor)$	ΔO	ΔI
$(2b, 2b)$	(b, b)	$+1$	0
$(2b+1, 2b)$	(b, b)	$+1$	0
$(2b+1, 2a+1)$	(b, a)	$+1$	-1
$(2a+1, 2a)$	(a, a)	-2	$+1$
$(2a, 2a)$	(a, a)	0	-1
$(2a, 2a+1)$	(a, a)	0	-1
$(2b, 2b+1)$	(b, b)	-2	$+2$
$(2b+1, 2a)$	(b, a)	0	-1

No other ordered pair is affected, hence every other pair contributes 0.

For brevity write

$$I_{aa} := I_S(a,a), \quad O_{aa} := O_S(a,a), \quad I_{bb} := I_S(b,b),$$
$$O_{bb} := O_S(b,b), \quad I_{ba} := I_S(b,a), \quad O_{ba} := O_S(b,a).$$

Using the table, the eight non-zero contributions to ΔN are:

$$\begin{aligned}
(2b, 2b): &\quad -2I_{bb},\\
(2b+1, 2b): &\quad -2I_{bb},\\
(2b+1, 2a+1): &\quad -2q + 2O_{ba} - 2I_{ba} + 1,\\
(2a+1, 2a): &\quad 2q - 2O_{aa} + 4I_{aa} + 2,\\
(2a, 2a): &\quad -2q + 2O_{aa},\\
(2a, 2a+1): &\quad -2q + 2O_{aa},\\
(2b, 2b+1): &\quad 4q - 4O_{bb} + 4I_{bb} + 4,\\
(2b+1, 2a): &\quad -2q + 2O_{ba}.
\end{aligned}$$

Summing them gives

$$\Delta N = -2I_{ba} + 4I_{aa} + 2O_{aa} + 4O_{ba} - 4O_{bb} - 2q + 7.$$

Now invoke the four degree relations contained in $H_q(a,b;S)$:

$$I_{aa} + O_{aa} = q, \qquad I_{bb} + O_{bb} = q, \qquad I_{bb} + O_{ba} = q - 1, \qquad I_{ba} + O_{aa} = q + 1.$$

From these we obtain

$$O_{aa} = q + 1 - I_{ba}, \qquad I_{aa} = I_{ba} - 1, \qquad O_{ba} = q - 1 - I_{bb}, \qquad O_{bb} = q - I_{bb}.$$

Substituting into the formula for ΔN,

$$\begin{aligned}
\Delta N &= -2I_{ba} + 4(I_{ba} - 1) + 2(q + 1 - I_{ba}) + 4(q - 1 - I_{bb}) - 4(q - I_{bb}) - 2q + 7\\
&= 1.
\end{aligned}$$

Therefore

$$N_{2q}(T) = N_{2q}(X) + 1 = 16N_q(S) + 1,$$

as claimed. □

3.2.1. *Propagation of the local hypothesis.* For $u = (u_1, u_2, u_3) \in [q]^3$, write

$$B(u) := \{(2u_1 + \varepsilon_1, 2u_2 + \varepsilon_2, 2u_3 + \varepsilon_3) : \varepsilon_1, \varepsilon_2, \varepsilon_3 \in \{0,1\}\} \subseteq [2q]^3.$$

We call $B(u)$ the *microcell above* u.

Proposition 15. *Let $S \subseteq [q]^3$, and let $a, b \in [q]$ with $a \neq b$. Assume that $H_q(a,b;S)$ holds. Let*

$$X := L_q(S) \subseteq [2q]^3,$$

and let $T \subseteq [2q]^3$ be obtained from X by the seven-site gadget above. Define

$$a' := 2a + 1, \qquad b' := 2b + 1.$$

Then

$$H_{2q}(a', b'; T)$$

holds.

Proof. All seven toggled sites lie in the four microcells above (a, a, a), (b, b, a), (b, a, a), and (b, b, b). We verify the four membership conditions and the four degree-balance conditions for the new pair $(a', b') = (2a + 1, 2b + 1)$.

1. Membership conditions.

Because $(a, a, a) \in S$, the whole microcell above (a, a, a) lies in X, hence

$$(a', a', a') = (2a + 1, 2a + 1, 2a + 1) \in X.$$

This site is not toggled, so $(a', a', a') \in T$.

Because $(b, b, a) \in S$, the whole microcell above (b, b, a) lies in X, hence

$$(b', b', a') = (2b + 1, 2b + 1, 2a + 1) \in X \subseteq T,$$

again because this site is not toggled.

Because $(b, a, a) \notin S$, the whole microcell above (b, a, a) is absent from X, so

$$(b', a', a') = (2b + 1, 2a + 1, 2a + 1) \notin X.$$

Among the three additions, only $P_3 = (2b + 1, 2a + 1, 2a)$ lies in that microcell, so (b', a', a') is still absent from T.

Because $(b, b, b) \notin S$, the whole microcell above (b, b, b) is absent from X, in particular

$$(b', b', b') = (2b + 1, 2b + 1, 2b + 1) \notin X.$$

The gadget adds only P_1 and P_2 in that microcell, so $(b', b', b') \notin T$.

Thus the membership part of $H_{2q}(a', b'; T)$ holds.

2. The identity $I_T(a', a') + O_T(a', a') = 2q$.

No toggled site has initial pair (a', a'), and no toggled site has terminal pair (a', a'). Therefore

$$I_T(a', a') = I_X(a', a') = 2I_S(a, a), \qquad O_T(a', a') = O_X(a', a') = 2O_S(a, a).$$

Using $I_S(a, a) + O_S(a, a) = q$, we obtain

$$I_T(a', a') + O_T(a', a') = 2q.$$

3. The identity $I_T(b', b') + O_T(b', b') = 2q$.

Exactly the same argument gives

$$I_T(b', b') = 2I_S(b, b), \qquad O_T(b', b') = 2O_S(b, b),$$

so from $I_S(b, b) + O_S(b, b) = q$ we get

$$I_T(b', b') + O_T(b', b') = 2q.$$

4. The identity $I_T(b', b') + O_T(b', a') = 2q - 1$.

We already know that $I_T(b', b') = 2I_S(b, b)$. Moreover, $O_T(b', a')$ counts triples of T whose first two coordinates are $(b', a') = (2b + 1, 2a + 1)$. In the lift X, this count is $2O_S(b, a)$. The gadget adds exactly one such triple, namely

$$P_3 = (2b + 1, 2a + 1, 2a),$$

and removes none with the same initial pair. Hence

$$O_T(b', a') = 2O_S(b, a) + 1.$$

Using $I_S(b, b) + O_S(b, a) = q - 1$, we conclude that

$$I_T(b', b') + O_T(b', a') = 2I_S(b, b) + 2O_S(b, a) + 1 = 2q - 1.$$

5. The identity $I_T(b', a') + O_T(a', a') = 2q + 1$.

We already know that $O_T(a', a') = 2O_S(a, a)$. On the other hand, $I_T(b', a')$ counts triples of T whose last two coordinates are $(b', a') = (2b + 1, 2a + 1)$. In the lift X, this count is $2I_S(b, a)$. The gadget removes exactly one such triple, namely

$$M_4 = (2b, 2b + 1, 2a + 1),$$

and adds none with the same terminal pair. Therefore

$$I_T(b', a') = 2I_S(b, a) - 1.$$

Using $I_S(b, a) + O_S(a, a) = q + 1$, we obtain

$$I_T(b', a') + O_T(a', a') = 2I_S(b, a) - 1 + 2O_S(a, a) = 2q + 1.$$

All four membership conditions and all four degree-balance conditions hold, so $H_{2q}(a', b'; T)$ follows. □

3.2.2. *The explicit base configuration at scale $q = 16$.* The lower-bound construction requires one explicit seed configuration $S_{16} \subseteq [16]^3$ satisfying a local compatibility hypothesis and having a sufficiently large value of N_{16}. The full specification of S_{16} is finite but bulky: it is described by ten fibres and a 16×16 fibre table. Since these data play a purely foundational role in the induction, we place the complete definition in Appendix A.1 and keep only the summary needed for the argument here.

More precisely, Appendix A.1 defines ten fibres

$$\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}, \mathcal{E}, \mathcal{F}, \mathcal{G}, \mathcal{H}, \mathcal{I}, \mathcal{J} \subseteq [16]$$

and a fibre table $(T_{a,b})_{(a,b)\in[16]^2}$ with values among these ten sets. The seed configuration is then

$$(a, b, c) \in S_{16} \quad \Longleftrightarrow \quad c \in T_{a,b}.$$

The choice $q = 16 = 2^4$ is the natural base scale for the construction: the propagation step is dyadic, so once a single admissible seed is available at one power of two, it propagates canonically to all larger dyadic scales. We have not attempted to optimise the smallest possible seed size; rather, $q = 16$ is the first scale at which we found a convenient explicit configuration with enough room to enforce the local hypothesis and achieve the target density.

The next lemma records exactly the two facts from this explicit dataset that are needed later: the base count and the local hypothesis required by the dyadic propagation. Their complete finite verification is given in Appendix A.

Lemma 16. *Let $S_{16} \subseteq [16]^3$ be the explicit set defined in Appendix A.1. Then:*

(1)
$$N_{16}(S_{16}) = 24849.$$

(2) *The local hypothesis $H_{16}(8, 14; S_{16})$ holds. Equivalently,*

$$(8, 8, 8) \in S_{16}, \qquad (14, 14, 8) \in S_{16}, \qquad (14, 8, 8) \notin S_{16}, \qquad (14, 14, 14) \notin S_{16},$$
$$I_{S_{16}}(8, 8) + O_{S_{16}}(8, 8) = 16,$$
$$I_{S_{16}}(14, 14) + O_{S_{16}}(14, 14) = 16,$$
$$I_{S_{16}}(14, 14) + O_{S_{16}}(14, 8) = 15,$$
$$I_{S_{16}}(14, 8) + O_{S_{16}}(8, 8) = 17.$$

Proof. The full finite verification is recorded in Appendix A. In brief, the four membership assertions are read directly from the fibre table, the four degree identities are obtained by counting the occurrences of the values 8 and 14 in the corresponding rows and columns, and the counting identity

$$N_{16}(S_{16}) = \sum_{u,v=0}^{15} I_{S_{16}}(u, v)\big(16 - O_{S_{16}}(u, v)\big)$$

is then evaluated from the complete incoming- and outgoing-degree matrices. The resulting row sums add up to 24849. □

3.2.3. *Inductive construction and the resulting lower bound.*

Proposition 17. *Set $q_m := 2^m$ for $m \geq 4$. Define*

$$S_{q_4} := S_{16}, \qquad a_4 := 8, \qquad b_4 := 14,$$

and recursively, for $m \geq 4$, let $S_{q_{m+1}} \subseteq [q_{m+1}]^3$ be obtained from S_{q_m} by first taking the dyadic lift and then applying the seven-site gadget with parameters (a_m, b_m). Set

$$a_{m+1} := 2a_m + 1, \qquad b_{m+1} := 2b_m + 1.$$

Then for every $m \geq 4$:

(1) *$H_{q_m}(a_m, b_m; S_{q_m})$ holds;*
(2)
$$N_{q_{m+1}}(S_{q_{m+1}}) = 16\, N_{q_m}(S_{q_m}) + 1;$$
(3)
$$N_{q_m}(S_{q_m}) = \frac{91}{240}\, q_m^4 - \frac{1}{15}.$$

Proof. The base lemma gives $H_{16}(8, 14; S_{16})$, so the claim in (1) holds for $m = 4$. If $H_{q_m}(a_m, b_m; S_{q_m})$ holds, then Proposition 15 gives

$$H_{q_{m+1}}(a_{m+1}, b_{m+1}; S_{q_{m+1}}),$$

which proves (1) for all $m \geq 4$ by induction.

Under the same inductive hypothesis, Lemma 14 yields

$$N_{q_{m+1}}(S_{q_{m+1}}) = 16\, N_{q_m}(S_{q_m}) + 1,$$

which is (2).

To solve the recurrence, use the initial value $N_{16}(S_{16}) = 24849$. Iterating (2) gives

$$N_{q_m}(S_{q_m}) = 16^{m-4} \cdot 24849 + \sum_{j=0}^{m-5} 16^j = 16^{m-4} \cdot 24849 + \frac{16^{m-4} - 1}{15}.$$

Since $q_m = 2^m$, so that $16^{m-4} = q_m^4/16^4 = q_m^4/65536$, and since

$$\frac{24849}{65536} + \frac{1}{15 \cdot 65536} = \frac{91}{240},$$

we obtain

$$N_{q_m}(S_{q_m}) = \frac{91}{240}\, q_m^4 - \frac{1}{15}.$$

This proves (3). □

Corollary 18.

$$\frac{3}{8} < \frac{91}{240} \leq \lambda_3 \leq \frac{11}{28} < \frac{2}{5}.$$

Proof. For each $m \geq 4$, let $A_m := A_{S_{q_m}} \subseteq [0,1]^3$ be the q_m-adic set associated with S_{q_m}. By Proposition 17 and the correspondence lemma,

$$\Phi(A_m) = \Lambda_{q_m}(S_{q_m}) = \frac{N_{q_m}(S_{q_m})}{q_m^4} = \frac{91}{240} - \frac{1}{15 q_m^4}.$$

Letting $m \to \infty$ gives

$$\lambda_3 \geq \frac{91}{240}.$$

The upper bound $\lambda_3 \leq 11/28$ is Corollary 12. The strict inequalities with $3/8$ and $2/5$ are immediate. □

3.3. **The independence number of $B(4,q)$.** We now combine Proposition 3, the asymptotic result of Section 2, and the explicit bounds for λ_3 established above.

Theorem 19. *As $q \to \infty$,*

$$\alpha(4,q) = \lambda_3 q^4 + o(q^4),$$

with

$$\frac{91}{240} \le \lambda_3 \le \frac{11}{28}.$$

Equivalently,

$$\frac{91}{240}q^4 + o(q^4) \le \alpha(4,q) \le \frac{11}{28}q^4 + o(q^4).$$

The same asymptotic estimate also holds for $\alpha_{\mathrm{loop}}(4,q)$.

Proof. The asymptotic formula is exactly Theorem 7 specialised to $k=4$. The upper bound for λ_3 is Corollary 12, and the lower bound is Corollary 18. Substituting these bounds into Theorem 7 yields the claim. □

Along the dyadic subsequence $q = 2^m$, Proposition 17 gives the sharper explicit bound

$$N_{2^m}(S_{2^m}) = \frac{91}{240}\,2^{4m} - \frac{1}{15}.$$

Therefore

$$\alpha_{\mathrm{loop}}(4,2^m) \ge \frac{91}{240}\,2^{4m} - \frac{1}{15}, \qquad \alpha(4,2^m) \ge \frac{91}{240}\,2^{4m} - \frac{1}{15}.$$

The universal upper bound from Proposition 11 reads

$$\alpha_{\mathrm{loop}}(4,q) \le \frac{11}{28}q^4, \qquad \alpha(4,q) \le \frac{11}{28}q^4 + q.$$

Remark 20 (Road map of the $k=4$ lower bound)**.** *The lower bound has four logically distinct layers. One starts from the explicit seed S_{16}, verifies finitely that it has the required local structure and that $N_{16}(S_{16}) = 24849$, propagates this information to all dyadic scales by the lift-plus-gadget construction, and finally passes from dyadic discrete sets to the continuum variational problem through the correspondence established in Section 2. This separation is useful for refereeing: only the first layer is finite bookkeeping, while the later steps are conceptual and remain unchanged once the base seed has been verified.*

4. Exact formulas for $k = 11, 13$

In this section we specialise to the binary graph underlying $B(k,2)$, where k is an odd prime. We write words as

$$x = x_0x_1\ldots x_{k-1} \in \{0,1\}^k,$$

and let

$$\rho(x_0x_1\ldots x_{k-1}) := x_1x_2\ldots x_{k-1}x_0$$

be the cyclic left rotation. Throughout this section, orbit indices are understood modulo k. We also write 0^k and 1^k for the two constant words. This is the only place in the paper where we switch to 0-based coordinate indexing, in order to align the notation with the cyclic rotation action.

Two results of Lichiardopol are the external input for what follows. First, the binary upper bound from [9, Section 4] gives

$$\alpha(k,2) \le 1 + \frac{k-1}{2k}(2^k - 2). \tag{6}$$

Second, by [9, Theorem 4.4], if the bound (6) is attained by an independent set containing at most one loop-vertex, then for every alphabet size $q \ge 2$ one has

$$\alpha(k,q) = \frac{(k-1)(q^k-q)}{2k} + 1, \qquad \alpha_{\mathrm{loop}}(k,q) = \frac{(k-1)(q^k-q)}{2k}. \tag{7}$$

Thus the binary problem controls the exact formulas for all $q \ge 2$.

4.1. **Rotation orbits and the phase reduction.** For $x \in \{0,1\}^k$, let

$$C(x) := \{\rho^i(x) : i \in \mathbb{Z}/k\mathbb{Z}\}$$

be its rotation orbit.

Lemma 21. *If $x \in \{0,1\}^k$ is non-constant, then $|C(x)| = k$.*

Proof. If $\rho^r(x) = x$ for some $r \in \mathbb{Z}/k\mathbb{Z}$, then x has cyclic period r. Since k is prime, every non-zero class in $\mathbb{Z}/k\mathbb{Z}$ generates the whole group, so a non-trivial period would force all coordinates of x to coincide. Hence a non-constant word has no non-trivial stabiliser under rotation, and its orbit has cardinality k. □

Lemma 22. *Let $x \in \{0,1\}^k$ be non-constant, and write $x^{(i)} := \rho^i(x)$ for $i \in \mathbb{Z}/k\mathbb{Z}$. Then the subgraph induced by $C(x)$ in the simple graph underlying $B(k,2)$ is the cycle graph C_k. Equivalently,*

$$x^{(i)} \sim x^{(j)} \qquad \Longleftrightarrow \qquad j - i \equiv \pm 1 \pmod{k}.$$

Proof. Because adjacency is invariant under simultaneous rotation of both words, it is enough to determine when $x^{(0)}$ is adjacent to $x^{(r)}$. If the suffix of length $k-1$ of $x^{(0)}$ equals the prefix of length $k-1$ of $x^{(r)}$, then x has cyclic period $r-1$; if the prefix of length $k-1$ of $x^{(0)}$ equals the suffix of length $k-1$ of $x^{(r)}$, then x has cyclic period $r+1$. Since x is non-constant and k is prime, Lemma 21 implies that only the trivial period can occur. Thus $r \equiv 1$ or $r \equiv -1 \pmod{k}$, and the claim follows. □

Let

$$J_k := \{1, 3, 5, \dots, k-2\} \subseteq \mathbb{Z}/k\mathbb{Z}.$$

For a non-trivial rotation orbit $C = (x^{(i)})_{i \in \mathbb{Z}/k\mathbb{Z}}$ and a phase $t \in \mathbb{Z}/k\mathbb{Z}$, define

$$A_t(C) := \{x^{(t+r)} : r \in J_k\}.$$

Lemma 23. *For every non-trivial rotation orbit C and every $t \in \mathbb{Z}/k\mathbb{Z}$, the set $A_t(C)$ is independent and has cardinality $(k-1)/2$.*

Proof. By Lemma 22, the only edges inside C join consecutive residues modulo k. The translate $J_k + t$ contains no two consecutive residues, hence $A_t(C)$ is independent. Its cardinality is $|J_k| = (k-1)/2$. □

Proposition 24. *Let $S \subseteq \{0,1\}^k$ be an independent set such that*

$$|S| = 1 + \frac{k-1}{2k}(2^k - 2)$$

and such that S contains exactly one loop-vertex. Then for every non-trivial rotation orbit C one has

$$|S \cap C| = \frac{k-1}{2},$$

and there exists a unique phase $t_C \in \mathbb{Z}/k\mathbb{Z}$ such that

$$S \cap C = A_{t_C}(C).$$

Proof. The $2^k - 2$ non-constant words split into

$$N_k := \frac{2^k - 2}{k}$$

non-trivial rotation orbits by Lemma 21. Since S contains exactly one loop-vertex and has cardinality

$$1 + \frac{k-1}{2} N_k,$$

its non-constant part has size exactly $\frac{k-1}{2} N_k$. By Lemma 22, each non-trivial orbit induces a copy of C_k, so it contributes at most $(k-1)/2$ vertices to S. Therefore every non-trivial orbit must attain this maximum. The k maximum independent sets of C_k are exactly the translates of the alternating pattern J_k. Hence there exists a unique phase $t_C \in \mathbb{Z}/k\mathbb{Z}$ such that $S \cap C = A_{t_C}(C)$. □

To express the compatibility constraints between different orbits, let $C = (x^{(i)})_{i\in\mathbb{Z}/k\mathbb{Z}}$ and $C' = (y^{(j)})_{j\in\mathbb{Z}/k\mathbb{Z}}$ be two non-trivial rotation orbits and define the adjacency-difference set

$$D(C, C') := \{j - i \pmod k : x^{(i)} \sim y^{(j)}\} \subseteq \mathbb{Z}/k\mathbb{Z}.$$

The corresponding forbidden phase-difference set is

$$F(C, C') := \{\delta - (b - a) \pmod k : \delta \in D(C, C'),\ a, b \in J_k\}.$$

If $\ell \in \{0^k, 1^k\}$ is a chosen loop-vertex and $C = (x^{(i)})_{i\in\mathbb{Z}/k\mathbb{Z}}$ is a non-trivial orbit, define also

$$D(\ell, C) := \{i \in \mathbb{Z}/k\mathbb{Z} : \ell \sim x^{(i)}\}$$

and

$$F(\ell, C) := \{\delta - a \pmod k : \delta \in D(\ell, C),\ a \in J_k\}.$$

Thus a phase t_C is compatible with ℓ precisely when $t_C \notin F(\ell, C)$.

Theorem 25. *Fix $\ell \in \{0^k, 1^k\}$. For each non-trivial rotation orbit C, choose a phase $t_C \in \mathbb{Z}/k\mathbb{Z}$ and set*

$$S_\ell(\{t_C\}) := \{\ell\} \cup \bigcup_C A_{t_C}(C),$$

where the union runs over all non-trivial rotation orbits. Then $S_\ell(\{t_C\})$ is independent if and only if the following two conditions hold:

(i) *for every non-trivial orbit C, one has $t_C \notin F(\ell, C)$;*
(ii) *for every pair of distinct non-trivial orbits C, C', one has*

$$t_{C'} - t_C \notin F(C, C').$$

Whenever these conditions are satisfied,

$$|S_\ell(\{t_C\})| = 1 + \frac{k-1}{2k}(2^k - 2).$$

Conversely, every independent set of this cardinality with exactly one loop-vertex arises in this way.

Proof. Lemma 23 shows that each set $A_{t_C}(C)$ is independent inside its own orbit. A cross-conflict between $A_{t_C}(C)$ and $A_{t_{C'}}(C')$ occurs if and only if there exist $a, b \in J_k$ such that $x^{(t_C+a)} \sim y^{(t_{C'}+b)}$, namely if and only if

$$(t_{C'} + b) - (t_C + a) \in D(C, C').$$

This is equivalent to $t_{C'} - t_C \in F(C, C')$, which gives condition (ii). Likewise, ℓ is adjacent to some vertex of $A_{t_C}(C)$ if and only if there exist $a \in J_k$ and $\delta \in D(\ell, C)$ such that $t_C + a \equiv \delta \pmod k$, namely if and only if $t_C \in F(\ell, C)$, which is condition (i). The cardinality formula follows from Lemma 23, and the converse is exactly Proposition 24. □

Remark 26. *The phase reduction converts the search for an extremal binary example with one prescribed loop-vertex into a finite difference-CSP on the non-trivial rotation orbits. This CSP is sparse for two elementary reasons. First, if $x \sim y$ in the simple graph underlying $B(k, 2)$, then the Hamming weights satisfy $|\mathrm{wt}(x) - \mathrm{wt}(y)| \le 1$. Hence only adjacent Hamming-weight layers can interact. Second, each binary word has at most four de Bruijn neighbours, so the orbit-conflict graph on the non-trivial rotation orbits has maximum degree at most $4k$.*

4.2. **Certificates and the cases $k = 11, 13$.** For the prime cases $k = 11$ and $k = 13$, we use a single *compact orbit-phase certificate*: for each non-trivial rotation orbit it records one canonical representative together with the corresponding phase t_C. From this data one reconstructs the entire candidate independent set. The two certificates used in this paper, together with a verifier script, are reproduced in Appendix B.

The role of the certificates is entirely finite and explicit. Starting from the compact orbit-phase file, one reconstructs every non-trivial orbit, selects the alternating positions indexed by $J_k + t_C$, takes the union together with 0^k, checks the target cardinality, verifies independence directly by testing the at most four de Bruijn neighbours of each selected vertex, and confirms that 1^k is

absent. Thus the computer-assisted part of Theorems 27 and 29 is a verification statement, not a search statement. For reproducibility, Appendix B records the certificate format, the verifier script, and the explicit certificate data used in the verification. The verifier uses only the Python standard library, and reads a single certificate file at a time; no external solver, random search, or hidden preprocessing is required.

Theorem 27. *One has*

$$\alpha(11,2) = 931.$$

More precisely, there exists an independent set in the simple graph underlying $B(11,2)$ *of cardinality* 931 *that contains* 0^{11} *and excludes* 1^{11}*.*

Proof. There are

$$N_{11} = \frac{2^{11}-2}{11} = 186$$

non-trivial rotation orbits, so the binary upper bound (6) gives

$$\alpha(11,2) \le 1 + \frac{10}{22}(2^{11}-2) = 1 + 5 \cdot 186 = 931.$$

The certificate for $k = 11$ records one phase for each of the 186 non-trivial rotation orbits. Applying the verification protocol described above reconstructs an independent set of cardinality 931 containing 0^{11} and excluding 1^{11}. Therefore the upper bound is attained, and $\alpha(11,2) = 931$. □

Corollary 28. *For every* $q \ge 2$*,*

$$\alpha(11,q) = \frac{5(q^{11}-q)}{11} + 1, \qquad \alpha_{\mathrm{loop}}(11,q) = \frac{5(q^{11}-q)}{11}.$$

Theorem 29. *One has*

$$\alpha(13,2) = 3781.$$

More precisely, there exists an independent set in the simple graph underlying $B(13,2)$ *of cardinality* 3781 *that contains* 0^{13} *and excludes* 1^{13}*.*

Proof. There are

$$N_{13} = \frac{2^{13}-2}{13} = 630$$

non-trivial rotation orbits, so the binary upper bound (6) gives

$$\alpha(13,2) \le 1 + \frac{12}{26}(2^{13}-2) = 1 + 6 \cdot 630 = 3781.$$

The certificate for $k = 13$ records one phase for each of the 630 non-trivial rotation orbits. Applying the verification protocol described above reconstructs an independent set of cardinality 3781 containing 0^{13} and excluding 1^{13}. Therefore the upper bound is sharp, and $\alpha(13,2) = 3781$. □

Corollary 30. *For every* $q \ge 2$*,*

$$\alpha(13,q) = \frac{6(q^{13}-q)}{13} + 1, \qquad \alpha_{\mathrm{loop}}(13,q) = \frac{6(q^{13}-q)}{13}.$$

Appendix A. Data and verification for $k = 4$, $q = 16$

This appendix incorporates the complete finite component of the lower-bound construction for $k = 4$ at the base scale $q = 16$. In parallel with Appendix B, we present the seed in a compact, uniform form: first the defining data, then the verification protocol and script, and finally the derived degree and contribution tables used in the computation of $N_{16}(S_{16})$.

A.1. **Seed data.**

A.1.1. *Named fibres.* We define ten fibres as subsets of [16]:

$$\begin{aligned}
\mathcal{A} &:= \varnothing,\\
\mathcal{B} &:= \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\},\\
\mathcal{C} &:= \{6,7\},\\
\mathcal{D} &:= \{2,3,6,7\},\\
\mathcal{E} &:= \{2,3,6,7,12,13\},\\
\mathcal{F} &:= \{2,3,6,7,8,9,12,13\},\\
\mathcal{G} &:= \{2,3,4,5,6,7,8,9,12,13,14,15\},\\
\mathcal{H} &:= \{2,3,6,7,8,9,12,13,14,15\},\\
\mathcal{I} &:= \{2,3,6,7,9,12,13\},\\
\mathcal{J} &:= \{2,3,6,7,8,9,12,13,14\}.
\end{aligned}$$

A.1.2. *Fibre table.* Define $S_{16} \subseteq [16]^3$ by

$$(a,b,c) \in S_{16} \quad \Longleftrightarrow \quad c \in T_{a,b},$$

where the fibre $T_{a,b}$ is selected from the following 16×16 label matrix:

$T_{a,b}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	$\mathcal{G}$	$\mathcal{G}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{G}$	$\mathcal{G}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$
1	$\mathcal{G}$	$\mathcal{G}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{G}$	$\mathcal{G}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$
2	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{B}$	$\mathcal{B}$
3	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{B}$	$\mathcal{B}$
4	$\mathcal{G}$	$\mathcal{G}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{H}$	$\mathcal{H}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{G}$	$\mathcal{G}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$
5	$\mathcal{G}$	$\mathcal{G}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{H}$	$\mathcal{H}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{G}$	$\mathcal{G}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$
6	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{B}$	$\mathcal{B}$
7	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{B}$	$\mathcal{B}$
8	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{F}$	$\mathcal{E}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{B}$	$\mathcal{B}$
9	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{B}$	$\mathcal{B}$
10	$\mathcal{G}$	$\mathcal{G}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{G}$	$\mathcal{G}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$
11	$\mathcal{G}$	$\mathcal{G}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{G}$	$\mathcal{G}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{A}$
12	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{B}$	$\mathcal{B}$
13	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{B}$	$\mathcal{B}$
14	$\mathcal{G}$	$\mathcal{G}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{H}$	$\mathcal{H}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{I}$	$\mathcal{E}$	$\mathcal{G}$	$\mathcal{G}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{F}$	$\mathcal{J}$
15	$\mathcal{G}$	$\mathcal{G}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{H}$	$\mathcal{H}$	$\mathcal{A}$	$\mathcal{A}$	$\mathcal{E}$	$\mathcal{E}$	$\mathcal{G}$	$\mathcal{G}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{E}$	$\mathcal{J}$

A.1.3. *Fibre cardinalities.* We recall the ten fibres used to define $S_{16} \subseteq [16]^3$:

$$\begin{aligned}
\mathcal{A} &:= \varnothing, & |\mathcal{A}| &= 0,\\
\mathcal{B} &:= [16], & |\mathcal{B}| &= 16,\\
\mathcal{C} &:= \{6,7\}, & |\mathcal{C}| &= 2,\\
\mathcal{D} &:= \{2,3,6,7\}, & |\mathcal{D}| &= 4,\\
\mathcal{E} &:= \{2,3,6,7,12,13\}, & |\mathcal{E}| &= 6,\\
\mathcal{F} &:= \{2,3,6,7,8,9,12,13\}, & |\mathcal{F}| &= 8,\\
\mathcal{G} &:= \{2,3,4,5,6,7,8,9,12,13,14,15\}, & |\mathcal{G}| &= 12,\\
\mathcal{H} &:= \{2,3,6,7,8,9,12,13,14,15\}, & |\mathcal{H}| &= 10,\\
\mathcal{I} &:= \{2,3,6,7,9,12,13\}, & |\mathcal{I}| &= 7,\\
\mathcal{J} &:= \{2,3,6,7,8,9,12,13,14\}, & |\mathcal{J}| &= 9.
\end{aligned}$$

Thus, for every pair $(a,b) \in [16]^2$, the outgoing degree is simply

$$O_{S_{16}}(a,b) = |T_{a,b}|.$$

This compact description is the complete defining data for the seed: all subsequent verifications are reconstructed from these ten named fibres and the 16×16 label matrix.

A.2. **Verification protocol.** The finite verification has three components: first one checks the local hypothesis $H_{16}(8,14;S_{16})$; next one computes the incoming and outgoing degree matrices; finally one evaluates the contribution matrix and the resulting count $N_{16}(S_{16})$. We begin with the local hypothesis. By inspection of the fibre table,

$$T_{8,8} = \mathcal{F} = \{2,3,6,7,8,9,12,13\},$$
$$T_{14,14} = \mathcal{F} = \{2,3,6,7,8,9,12,13\},$$
$$T_{14,8} = \mathcal{I} = \{2,3,6,7,9,12,13\}.$$

Therefore

$$(8,8,8) \in S_{16}, \qquad (14,14,8) \in S_{16}, \qquad (14,8,8) \notin S_{16}, \qquad (14,14,14) \notin S_{16}.$$

Moreover,

$$O_{S_{16}}(8,8) = |\mathcal{F}| = 8, \qquad O_{S_{16}}(14,14) = |\mathcal{F}| = 8, \qquad O_{S_{16}}(14,8) = |\mathcal{I}| = 7.$$

To compute the relevant incoming degrees, recall that

$$I_{S_{16}}(u,v) = \#\{x \in [16] : (x,u,v) \in S_{16}\} = \#\{x \in [16] : v \in T_{x,u}\}.$$

Hence:

- $I_{S_{16}}(8,8)$ is the number of rows x such that $8 \in T_{x,8}$. Reading the eighth column of the fibre table, this happens for
$$x \in \{2,3,6,7,8,9,12,13\},$$
so $I_{S_{16}}(8,8) = 8$.
- $I_{S_{16}}(14,14)$ is the number of rows x such that $14 \in T_{x,14}$. Reading the fourteenth column of the fibre table, this happens for
$$x \in \{2,3,6,7,8,9,12,13\},$$
so $I_{S_{16}}(14,14) = 8$.
- $I_{S_{16}}(14,8)$ is the number of rows x such that $8 \in T_{x,14}$. Reading the fourteenth column of the fibre table and checking where the value 8 occurs, this happens for
$$x \in \{2,3,6,7,8,9,12,13,14\},$$
so $I_{S_{16}}(14,8) = 9$.

Consequently,

$$I_{S_{16}}(8,8) + O_{S_{16}}(8,8) = 8+8 = 16,$$
$$I_{S_{16}}(14,14) + O_{S_{16}}(14,14) = 8+8 = 16,$$
$$I_{S_{16}}(14,14) + O_{S_{16}}(14,8) = 8+7 = 15,$$
$$I_{S_{16}}(14,8) + O_{S_{16}}(8,8) = 9+8 = 17.$$

This proves the full local hypothesis $H_{16}(8,14;S_{16})$.

The script in the next subsection implements the same checks directly from the defining fibre table and also computes the matrices used later in this appendix.

A.3. **Verifier script.** To make the finite verification of the seed S_{16} independently checkable, we record here a short Python script that reconstructs the fibre table, computes the incoming and outgoing degree matrices, verifies the local hypothesis $H_{16}(8,14;S_{16})$, and evaluates the count

$$N_{16}(S_{16}) = \#\{(a,b,c,d) \in [16]^4 : (a,b,c) \in S_{16},\ (b,c,d) \notin S_{16}\}.$$

When run exactly as printed below, the script outputs

$$O(8,8) = 8,\ I(8,8) = 8,\ O(14,14) = 8,\ I(14,14) = 8,\ O(14,8) = 7,\ I(14,8) = 9,$$

and finally

$$H_{16}(8,14;S_{16}) \text{ holds}, \qquad N_{16}(S_{16}) = 24849.$$

```
Q = 16

fibres = {
    "A": set(),
    "B": set(range(16)),
    "C": {6, 7},
    "D": {2, 3, 6, 7},
    "E": {2, 3, 6, 7, 12, 13},
    "F": {2, 3, 6, 7, 8, 9, 12, 13},
    "G": {2, 3, 4, 5, 6, 7, 8, 9, 12, 13, 14, 15},
    "H": {2, 3, 6, 7, 8, 9, 12, 13, 14, 15},
    "I": {2, 3, 6, 7, 9, 12, 13},
    "J": {2, 3, 6, 7, 8, 9, 12, 13, 14},
}

labels = [
    ["G","G","A","A","A","A","A","A","A","A","G","G","A","A","A","A"],
    ["G","G","A","A","A","A","A","A","A","A","G","G","A","A","A","A"],
    ["B","B","F","F","B","B","A","A","F","F","B","B","F","F","B","B"],
    ["B","B","F","F","B","B","A","A","F","F","B","B","F","F","B","B"],
    ["G","G","C","C","H","H","A","A","D","D","G","G","D","D","D","D"],
    ["G","G","C","C","H","H","A","A","D","D","G","G","D","D","D","D"],
    ["B","B","F","F","B","B","F","F","F","F","B","B","F","F","B","B"],
    ["B","B","F","F","B","B","F","F","F","F","B","B","F","F","B","B"],
    ["B","B","C","C","B","B","A","A","F","E","B","B","D","D","B","B"],
    ["B","B","C","C","B","B","A","A","F","F","B","B","D","D","B","B"],
    ["G","G","A","A","A","A","A","A","A","A","G","G","A","A","A","A"],
    ["G","G","A","A","A","A","A","A","A","A","G","G","A","A","A","A"],
    ["B","B","C","C","B","B","A","A","F","F","B","B","F","F","B","B"],
    ["B","B","C","C","B","B","A","A","F","F","B","B","F","F","B","B"],
    ["G","G","C","C","H","H","A","A","I","E","G","G","D","D","F","J"],
    ["G","G","C","C","H","H","A","A","E","E","G","G","D","D","E","J"],
]

T = [[fibres[name] for name in row] for row in labels]

# Outgoing and incoming degree matrices.
O = [[len(T[a][b]) for b in range(Q)] for a in range(Q)]
I = [[sum(1 for x in range(Q) if v in T[x][u]) for v in range(Q)] for u in range(Q)]

# Local hypothesis H_16(8,14; S_16).
assert 8 in T[8][8]
assert 8 in T[14][14]
assert 8 not in T[14][8]
assert 14 not in T[14][14]
assert I[8][8] + O[8][8] == 16
assert I[14][14] + O[14][14] == 16
assert I[14][14] + O[14][8] == 15
assert I[14][8] + O[8][8] == 17

print(f"O(8,8)={O[8][8]},␣I(8,8)={I[8][8]}")
print(f"O(14,14)={O[14][14]},␣I(14,14)={I[14][14]}")
print(f"O(14,8)={O[14][8]},␣I(14,8)={I[14][8]}")
print("H_16(8,14;S_16)␣holds")
```

```
# Count N_16(S_16).
N = 0
for a in range(Q):
    for b in range(Q):
        for c in T[a][b]:
            for d in range(Q):
                if d not in T[b][c]:
                    N += 1

print(f"N_16(S_16)={N}")
assert N == 24849
```

A.4. **Derived degree tables.** For convenience we record the matrices

$$O_{16}(u,v) := O_{S_{16}}(u,v), \qquad I_{16}(u,v) := I_{S_{16}}(u,v), \qquad u,v \in [16].$$

They are listed row by row below.

Table 1: The outgoing-degree matrix $O_{16}(u,v) = |T_{u,v}|$.

$u\backslash v$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	12	0	0	0	0	0	0	0	0	12	12	0	0	0	0
1	12	12	0	0	0	0	0	0	0	0	12	12	0	0	0	0
2	16	16	8	8	16	16	0	0	8	8	16	16	8	8	16	16
3	16	16	8	8	16	16	0	0	8	8	16	16	8	8	16	16
4	12	12	2	2	10	10	0	0	4	4	12	12	4	4	4	4
5	12	12	2	2	10	10	0	0	4	4	12	12	4	4	4	4
6	16	16	8	8	16	16	8	8	8	8	16	16	8	8	16	16
7	16	16	8	8	16	16	8	8	8	8	16	16	8	8	16	16
8	16	16	2	2	16	16	0	0	8	6	16	16	4	4	16	16
9	16	16	2	2	16	16	0	0	8	8	16	16	4	4	16	16
10	12	12	0	0	0	0	0	0	0	0	12	12	0	0	0	0
11	12	12	0	0	0	0	0	0	0	0	12	12	0	0	0	0
12	16	16	2	2	16	16	0	0	8	8	16	16	8	8	16	16
13	16	16	2	2	16	16	0	0	8	8	16	16	8	8	16	16
14	12	12	2	2	10	10	0	0	7	6	12	12	4	4	8	9
15	12	12	2	2	10	10	0	0	6	6	12	12	4	4	6	9

Table 2: The incoming-degree matrix $I_{16}(u,v) = \#\{x \in [16] : (x,u,v) \in S_{16}\}$.

$u\backslash v$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	8	8	16	16	16	16	16	16	16	16	8	8	16	16	16	16
1	8	8	16	16	16	16	16	16	16	16	8	8	16	16	16	16
2	0	0	4	4	0	0	12	12	4	4	0	0	4	4	0	0
3	0	0	4	4	0	0	12	12	4	4	0	0	4	4	0	0
4	8	8	12	12	8	8	12	12	12	12	8	8	12	12	12	12
5	8	8	12	12	8	8	12	12	12	12	8	8	12	12	12	12
6	0	0	2	2	0	0	2	2	2	2	0	0	2	2	0	0
7	0	0	2	2	0	0	2	2	2	2	0	0	2	2	0	0
8	0	0	12	12	0	0	12	12	8	9	0	0	10	10	0	0
9	0	0	12	12	0	0	12	12	7	7	0	0	10	10	0	0
10	8	8	16	16	16	16	16	16	16	16	8	8	16	16	16	16
11	8	8	16	16	16	16	16	16	16	16	8	8	16	16	16	16
12	0	0	12	12	0	0	12	12	6	6	0	0	6	6	0	0
13	0	0	12	12	0	0	12	12	6	6	0	0	6	6	0	0
14	8	8	12	12	8	8	12	12	9	9	8	8	10	10	8	8
15	8	8	12	12	8	8	12	12	10	10	8	8	10	10	10	8

A.5. **Contribution table and the computation of $N_{16}(S_{16})$.** The counting identity used in the proof of the base lemma is

$$N_{16}(S_{16}) = \sum_{u,v=0}^{15} I_{16}(u,v)\big(16 - O_{16}(u,v)\big).$$

Define the entrywise contribution matrix

$$C_{16}(u,v) := I_{16}(u,v)\big(16 - O_{16}(u,v)\big).$$

Using Tables 1 and 2, one obtains the following matrix.

Table 3: The contribution matrix $C_{16}(u,v) = I_{16}(u,v)(16 - O_{16}(u,v))$.

$u\backslash v$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	32	32	256	256	256	256	256	256	256	256	32	32	256	256	256	256
1	32	32	256	256	256	256	256	256	256	256	32	32	256	256	256	256
2	0	0	32	32	0	0	192	192	32	32	0	0	32	32	0	0
3	0	0	32	32	0	0	192	192	32	32	0	0	32	32	0	0
4	32	32	168	168	48	48	192	192	144	144	32	32	144	144	144	144
5	32	32	168	168	48	48	192	192	144	144	32	32	144	144	144	144
6	0	0	16	16	0	0	16	16	16	16	0	0	16	16	0	0
7	0	0	16	16	0	0	16	16	16	16	0	0	16	16	0	0
8	0	0	168	168	0	0	192	192	64	90	0	0	120	120	0	0
9	0	0	168	168	0	0	192	192	56	56	0	0	120	120	0	0
10	32	32	256	256	256	256	256	256	256	256	32	32	256	256	256	256
11	32	32	256	256	256	256	256	256	256	256	32	32	256	256	256	256
12	0	0	168	168	0	0	192	192	48	48	0	0	48	48	0	0
13	0	0	168	168	0	0	192	192	48	48	0	0	48	48	0	0
14	32	32	168	168	48	48	192	192	81	90	32	32	120	120	64	56
15	32	32	168	168	48	48	192	192	100	100	32	32	120	120	100	56

Summing each row of C_{16} gives

$$\begin{aligned}(r_0,\dots,r_{15}) = (&3200, 3200, 576, 576, 1808, 1808, 128, 128,\\ &1114, 1072, 3200, 3200, 912, 912, 1475, 1540).\end{aligned}$$

Finally,

$$\begin{aligned}N_{16}(S_{16}) &= 3200 + 3200 + 576 + 576 + 1808 + 1808 + 128 + 128\\ &\quad + 1114 + 1072 + 3200 + 3200 + 912 + 912 + 1475 + 1540\\ &= 24849.\end{aligned}$$

Appendix B. Data and verification for $k = 11, 13$

This appendix incorporates the complete computer-assisted component of Theorems 27 and 29 in a compact, uniform form. In parallel with Appendix A, we present first the defining data format, then the verification protocol and verifier script, and finally the certificate data themselves.

B.1. **Certificate data.** For a fixed prime length $k \in \{11, 13\}$, the certificate is a plain-text file with:

- a one-line header specifying k, the target cardinality, the mandatory included vertex 0^k, and the mandatory excluded vertex 1^k;
- one entry `representative:phase` for each non-trivial rotation orbit, where the representative is the lexicographically least binary word in the orbit and the phase is an integer in $\{0, \dots, k-1\}$;
- four such entries per line, purely for compactness of presentation.

Given such a certificate, the selected vertices on the orbit of a representative x are the rotations

$$\mathrm{rot}^{t+a}(x), \qquad a \in J_k = \{1, 3, \dots, k-2\},$$

where t is the certified phase for that orbit.

Thus the same file format works for both $k = 11$ and $k = 13$, and no auxiliary vertex list is needed: the full independent set is reconstructed directly from the orbit-phase data.

B.2. **Verification protocol.** The verification procedure is finite and explicit:

(1) parse the certificate header and the list of orbit-phase entries;
(2) check that every representative is canonical and generates a non-trivial orbit of size k;
(3) reconstruct the selected vertices on each orbit by the alternating pattern $J_k + t$;
(4) add the mandatory loop-vertex 0^k and verify that the total size is the target size;
(5) verify directly that no selected vertex is adjacent to another selected vertex in the underlying simple de Bruijn graph;
(6) verify that 1^k is not selected.

The following script implements exactly this protocol.

B.3. **Verifier script.**

```
#!/usr/bin/env python3
from __future__ import annotations

import re
import sys
from pathlib import Path

PAIR_RE = re.compile(r'([01]+):(\d+)')
HEADER_RE = re.compile(
    r'#\s*CERTIFICATE\s+k=(\d+)\s+target_size=(\d+)\s+include=([01]+)\s+exclude=([01]+)'
)


def rotate(word: str, shift: int = 1) -> str:
    shift %= len(word)
    return word[shift:] + word[:shift]


def parse_certificate(path: Path):
    lines = path.read_text().splitlines()
    if not lines:
        raise ValueError('empty certificate file')
    m = HEADER_RE.fullmatch(lines[0].strip())
    if not m:
        raise ValueError('invalid header in certificate file')
    k = int(m.group(1))
    target = int(m.group(2))
    include_word = m.group(3)
    exclude_word = m.group(4)
    if len(include_word) != k or len(exclude_word) != k:
        raise ValueError('header words have the wrong length')
    entries = []
    for line in lines[1:]:
        line = line.strip()
        if not line or line.startswith('#'):
            continue
        for rep, phase_str in PAIR_RE.findall(line):
            if len(rep) != k:
                raise ValueError(f'wrong representative length: {rep}')
            phase = int(phase_str)
            if not (0 <= phase < k):
                raise ValueError(f'phase out of range for {rep}: {phase}')
            entries.append((rep, phase))
    return k, target, include_word, exclude_word, entries


def canonical_rotation(word: str) -> str:
    rots = [rotate(word, i) for i in range(len(word))]
    return min(rots)


def orbit_from_rep(rep: str):
    seen = []
    cur = rep
    while cur not in seen:
        seen.append(cur)
```

```
        cur = rotate(cur, 1)
    return seen


def neighbors(word: str):
    k = len(word)
    left = word[1:]
    right = word[:-1]
    out = {left + bit for bit in '01'}
    out.update({bit + right for bit in '01'})
    out.discard(word)
    return out


def verify(path: Path) -> int:
    k, target, include_word, exclude_word, entries = parse_certificate(path)
    expected_orbits = (2**k - 2) // k
    if len(entries) != expected_orbits:
        raise ValueError(
            f'expected {expected_orbits} orbit entries, found {len(entries)}'
        )

    orbit_reps_seen = set()
    selected = {include_word}
    J = list(range(1, k, 2))

    for rep, phase in entries:
        if canonical_rotation(rep) != rep:
            raise ValueError(f'representative is not canonical: {rep}')
        orbit = orbit_from_rep(rep)
        if len(orbit) != k:
            raise ValueError(f'nontrivial orbit has wrong size for {rep}')
        if rep in orbit_reps_seen:
            raise ValueError(f'duplicate orbit representative: {rep}')
        orbit_reps_seen.add(rep)
        picks = {(phase + a) % k for a in J}
        for idx in picks:
            selected.add(orbit[idx])

    if exclude_word in selected:
        raise ValueError(f'excluded word {exclude_word} was selected')
    if len(selected) != target:
        raise ValueError(f'wrong size: expected {target}, found {len(selected)}')

    selected_set = set(selected)
    for word in selected:
        for nb in neighbors(word):
            if nb in selected_set:
                raise ValueError(f'adjacent selected vertices found: {word} ~ {nb}')

    print(f'OK: k={k}, selected={len(selected)}, nontrivial_orbits={len(entries)}')
    return 0


if __name__ == '__main__':
    if len(sys.argv) != 2:
        print(f'usage: {Path(sys.argv[0]).name} CERTIFICATE.txt', file=sys.stderr)
        sys.exit(2)
    sys.exit(verify(Path(sys.argv[1])))
```

B.4. **Certificate for $k = 11$.**

```
# CERTIFICATE k=11 target_size=931 include=00000000000 exclude=11111111111
# format: representative:phase (four entries per line)
00000000001:0 00000000011:0 00000000101:0 00000000111:0
00000001001:4 00000001011:4 00000001101:0 00000001111:6
00000010001:9 00000010011:9 00000010101:0 00000010111:0
00000011001:0 00000011011:4 00000011101:0 00000011111:0
00000100001:2 00000100011:4 00000100101:2 00000100111:0
00000101001:4 00000101011:6 00000101101:2 00000101111:6
00000110001:0 00000110011:0 00000110101:9 00000110111:9
```

```
00000111001:4 00000111011:4 00000111101:0 00000111111:4
00001000011:7 00001000101:9 00001000111:7 00001001001:7
00001001011:5 00001001101:9 00001001111:10 00001010001:7
00001010011:7 00001010101:9 00001010111:7 00001011001:7
00001011011:7 00001011101:9 00001011111:7 00001100011:4
00001100101:0 00001100111:0 00001101001:4 00001101011:6
00001101101:2 00001101111:6 00001110001:0 00001110011:0
00001110101:0 00001110111:0 00001111001:0 00001111011:0
00001111101:0 00001111111:0 00010001001:4 00010001011:4
00010001101:0 00010001111:4 00010010011:0 00010010101:0
00010010111:0 00010011001:2 00010011011:4 00010011101:0
00010011111:0 00010100011:4 00010100101:2 00010100111:2
00010101001:6 00010101011:4 00010101101:2 00010101111:6
00010110011:4 00010110101:0 00010110111:0 00010111001:4
00010111011:4 00010111101:2 00010111111:4 00011000111:9
00011001001:2 00011001011:4 00011001101:0 00011001111:4
00011010011:7 00011010101:7 00011010111:7 00011011001:7
00011011011:7 00011011101:7 00011011111:7 00011100101:2
00011100111:2 00011101001:6 00011101011:4 00011101101:2
00011101111:6 00011110011:4 00011110101:0 00011110111:0
00011111001:2 00011111011:4 00011111101:0 00011111111:2
00100100101:0 00100100111:0 00100101011:8 00100101101:0
00100101111:8 00100110011:3 00100110101:9 00100110111:7
00100111011:8 00100111101:2 00100111111:8 00101001011:3
00101001101:7 00101001111:1 00101010011:5 00101010101:9
00101010111:7 00101011011:5 00101011101:9 00101011111:5
00101100111:9 00101101011:8 00101101101:0 00101101111:8
00101110011:3 00101110101:9 00101110111:7 00101111011:3
00101111101:9 00101111111:3 00110011011:10 00110011101:9
00110011111:5 00110100111:2 00110101011:8 00110101101:2
00110101111:6 00110110101:0 00110110111:0 00110111011:8
00110111101:2 00110111111:6 00111001111:1 00111010101:7
00111010111:7 00111011011:5 00111011101:7 00111011111:5
00111101011:10 00111101101:7 00111101111:10 00111110101:9
00111110111:7 00111111011:10 00111111101:9 00111111111:3
01010101011:4 01010101111:6 01010110111:0 01010111011:4
01010111111:2 01011010111:9 01011011011:2 01011011111:9
01011101111:6 01011110111:2 01011111011:2 01011111111:2
01101101111:8 01101110111:7 01101111111:5 01110111111:2
01111011111:0 01111111111:0
```

B.5. **Certificate for $k = 13$.**

```
# CERTIFICATE k=13 target_size=3781 include=0000000000000 exclude=1111111111111
# format: representative:phase (four entries per line)
0000000000001:0 0000000000011:10 0000000000101:0 0000000000111:0
0000000001001:6 0000000001011:10 0000000001101:0 0000000001111:10
0000000010001:9 0000000010011:5 0000000010101:9 0000000010111:9
0000000011001:9 0000000011011:12 0000000011101:9 0000000011111:7
0000000100001:0 0000000100011:10 0000000100101:0 0000000100111:0
0000000101001:6 0000000101011:10 0000000101101:4 0000000101111:10
0000000110001:2 0000000110011:12 0000000110101:11 0000000110111:9
0000000111001:6 0000000111011:12 0000000111101:2 0000000111111:12
0000001000001:0 0000001000011:10 0000001000101:0 0000001000111:0
0000001001001:0 0000001001011:10 0000001001101:0 0000001001111:10
0000001010001:9 0000001010011:7 0000001010101:9 0000001010111:9
0000001011001:9 0000001011011:3 0000001011101:9 0000001011111:7
0000001100001:11 0000001100011:3 0000001100101:11 0000001100111:9
0000001101001:6 0000001101011:10 0000001101101:4 0000001101111:10
0000001110001:11 0000001110011:5 0000001110101:9 0000001110111:9
0000001111001:11 0000001111011:3 0000001111101:9 0000001111111:7
0000010000011:8 0000010000101:0 0000010000111:0 0000010001001:6
0000010001011:8 0000010001101:0 0000010001111:6 0000010010001:2
0000010010011:6 0000010010101:11 0000010010111:11 0000010011001:2
0000010011011:8 0000010011101:0 0000010011111:0 0000010100001:6
0000010100011:8 0000010100101:0 0000010100111:4 0000010101001:8
0000010101011:8 0000010101101:4 0000010101111:6 0000010110001:6
0000010110011:8 0000010110101:0 0000010110111:2 0000010111001:6
0000010111011:8 0000010111101:6 0000010111111:6 0000011000011:8
0000011000101:0 0000011000111:0 0000011001001:4 0000011001011:10
0000011001101:0 0000011001111:6 0000011010001:9 0000011010011:9
```

0000011010101:11 0000011010111:11 0000011011001:9 0000011011011:3
0000011011101:11 0000011011111:11 0000011100001:4 0000011100011:8
0000011100101:2 0000011100111:4 0000011101001:8 0000011101011:10
0000011101101:4 0000011101111:6 0000011110001:2 0000011110011:8
0000011110101:0 0000011110111:0 0000011111001:4 0000011111011:10
0000011111101:4 0000011111111:4 0000100001001:10 0000100001011:10
0000100001101:0 0000100001111:10 0000100010001:7 0000100010011:5
0000100010101:9 0000100010111:9 0000100011001:5 0000100011011:12
0000100011101:9 0000100011111:9 0000100100011:1 0000100100101:11
0000100100111:11 0000100101001:10 0000100101011:10 0000100101101:4
0000100101111:8 0000100110001:5 0000100110011:5 0000100110101:11
0000100110111:11 0000100111001:10 0000100111011:10 0000100111101:2
0000100111111:6 0000101000011:5 0000101000101:9 0000101000111:7
0000101001001:5 0000101001011:12 0000101001101:7 0000101001111:5
0000101010001:7 0000101010011:7 0000101010101:9 0000101010111:9
0000101011001:5 0000101011011:3 0000101011101:7 0000101011111:9
0000101100011:5 0000101100101:9 0000101100111:7 0000101101001:3
0000101101011:12 0000101101101:7 0000101101111:3 0000101110001:7
0000101110011:5 0000101110101:9 0000101110111:9 0000101111001:5
0000101111011:3 0000101111101:7 0000101111111:9 0000110000111:9
0000110001001:10 0000110001011:12 0000110001101:11 0000110001111:12
0000110010001:9 0000110010011:3 0000110010101:9 0000110010111:9
0000110011001:5 0000110011011:12 0000110011101:9 0000110011111:9
0000110100011:8 0000110100101:0 0000110100111:2 0000110101001:10
0000110101011:8 0000110101101:4 0000110101111:8 0000110110001:6
0000110110011:8 0000110110101:0 0000110110111:2 0000110111001:10
0000110111011:8 0000110111101:6 0000110111111:6 0000111000101:9
0000111000111:9 0000111001001:5 0000111001011:1 0000111001101:9
0000111001111:3 0000111010001:9 0000111010011:7 0000111010101:9
0000111010111:9 0000111011001:5 0000111011011:3 0000111011101:9
0000111011111:9 0000111100011:5 0000111100101:11 0000111100111:9
0000111101001:10 0000111101011:10 0000111101101:0 0000111101111:10
0000111110001:9 0000111110011:5 0000111110101:9 0000111110111:9
0000111111001:5 0000111111011:3 0000111111101:9 0000111111111:9
0001000100011:4 0001000100101:0 0001000100111:0 0001000101001:8
0001000101011:8 0001000101101:6 0001000101111:6 0001000110011:4
0001000110101:0 0001000110111:0 0001000111001:6 0001000111011:8
0001000111101:0 0001000111111:6 0001001000101:11 0001001000111:11
0001001001001:2 0001001001011:10 0001001001101:0 0001001001111:4
0001001010011:9 0001001010101:11 0001001010111:11 0001001011001:9
0001001011011:3 0001001011101:11 0001001011111:11 0001001100011:4
0001001100101:0 0001001100111:0 0001001101001:8 0001001101011:10
0001001101101:4 0001001101111:6 0001001110011:9 0001001110101:11
0001001110111:9 0001001111001:9 0001001111011:1 0001001111101:11
0001001111111:9 0001010001011:8 0001010001101:2 0001010001111:6
0001010010011:4 0001010010101:0 0001010010111:0 0001010011001:2
0001010011011:6 0001010011101:0 0001010011111:0 0001010100011:4
0001010100101:0 0001010100111:2 0001010101001:8 0001010101011:6
0001010101101:6 0001010101111:6 0001010110011:4 0001010110101:0
0001010110111:2 0001010111001:6 0001010111011:8 0001010111101:4
0001010111111:6 0001011000111:2 0001011001001:4 0001011001011:8
0001011001101:0 0001011001111:4 0001011010011:2 0001011010101:11
0001011010111:11 0001011011001:0 0001011011011:6 0001011011101:2
0001011011111:2 0001011100011:4 0001011100101:0 0001011100111:2
0001011101001:8 0001011101011:6 0001011101101:4 0001011101111:6
0001011110011:4 0001011110101:0 0001011110111:2 0001011111001:4
0001011111011:8 0001011111101:4 0001011111111:4 0001100011001:9
0001100011011:12 0001100011101:9 0001100011111:7 0001100100101:0
0001100100111:2 0001100101001:8 0001100101011:10 0001100101101:6
0001100101111:10 0001100110011:0 0001100110101:0 0001100110111:0
0001100111001:6 0001100111011:10 0001100111101:2 0001100111111:10
0001101000111:9 0001101001001:7 0001101001011:12 0001101001101:9
0001101001111:7 0001101010011:7 0001101010101:9 0001101010111:9
0001101011001:9 0001101011011:3 0001101011101:9 0001101011111:7
0001101100101:9 0001101100111:9 0001101101001:3 0001101101011:12
0001101101101:9 0001101101111:1 0001101110011:7 0001101110101:9
0001101110111:9 0001101111001:9 0001101111011:1 0001101111101:9
0001101111111:7 0001110001111:6 0001110010011:4 0001110010101:0
0001110010111:0 0001110011001:2 0001110011011:8 0001110011101:0
0001110011111:0 0001110100101:2 0001110100111:4 0001110101001:8

```
0001110101011:10 0001110101101:6 0001110101111:8 0001110110011:4
0001110110101:0 0001110110111:0 0001110111001:6 0001110111011:10
0001110111101:4 0001110111111:6 0001111001001:2 0001111001011:10
0001111001101:0 0001111001111:4 0001111010011:9 0001111010101:9
0001111010111:9 0001111011001:9 0001111011011:12 0001111011101:9
0001111011111:9 0001111100101:2 0001111100111:2 0001111101001:8
0001111101011:8 0001111101101:0 0001111101111:8 0001111110011:4
0001111110101:0 0001111110111:0 0001111111001:2 0001111111011:8
0001111111101:2 0001111111111:2 0010010010011:1 0010010010101:11
0010010010111:9 0010010011011:12 0010010011101:11 0010010011111:9
0010010100101:2 0010010100111:4 0010010101011:10 0010010101101:6
0010010101111:8 0010010110011:8 0010010110101:2 0010010110111:2
0010010111011:10 0010010111101:6 0010010111111:6 0010011001011:10
0010011001101:0 0010011001111:8 0010011010011:5 0010011010101:9
0010011010111:9 0010011011011:3 0010011011101:9 0010011011111:9
0010011100101:2 0010011100111:4 0010011101011:10 0010011101101:6
0010011101111:8 0010011110011:10 0010011110101:0 0010011110111:0
0010011111011:10 0010011111101:6 0010011111111:6 0010100101011:12
0010100101101:12 0010100101111:12 0010100110011:5 0010100110101:5
0010100110111:5 0010100111011:12 0010100111101:5 0010100111111:12
0010101001011:12 0010101001101:5 0010101001111:5 0010101010011:5
0010101010101:5 0010101010111:5 0010101011011:3 0010101011101:7
0010101011111:7 0010101100111:5 0010101101011:12 0010101101101:3
0010101101111:3 0010101110011:5 0010101110101:5 0010101110111:5
0010101111011:3 0010101111101:5 0010101111111:5 0010110010111:5
0010110011011:12 0010110011101:7 0010110011111:7 0010110100111:7
0010110101011:12 0010110101101:12 0010110101111:12 0010110110011:12
0010110110101:5 0010110110111:5 0010110111011:1 0010110111101:3
0010110111111:1 0010111001101:5 0010111001111:3 0010111010011:5
0010111010101:5 0010111010111:5 0010111011011:3 0010111011101:7
0010111011111:7 0010111100111:5 0010111101011:12 0010111101101:5
0010111101111:1 0010111110011:3 0010111110101:5 0010111110111:5
0010111111011:3 0010111111101:5 0010111111111:5 0011001100111:0
0011001101011:10 0011001101101:6 0011001101111:10 0011001110101:11
0011001110111:9 0011001111011:1 0011001111101:11 0011001111111:5
0011010011011:6 0011010011101:0 0011010011111:0 0011010100111:2
0011010101011:6 0011010101101:8 0011010101111:8 0011010110101:0
0011010110111:2 0011010111011:6 0011010111101:6 0011010111111:8
0011011001111:6 0011011010101:11 0011011010111:11 0011011011011:6
0011011011101:0 0011011011111:0 0011011100111:2 0011011101011:6
0011011101101:8 0011011101111:8 0011011110101:0 0011011110111:0
0011011111011:6 0011011111101:4 0011011111111:8 0011100111011:12
0011100111101:9 0011100111111:12 0011101001111:5 0011101010101:9
0011101010111:7 0011101011011:3 0011101011101:7 0011101011111:5
0011101101011:12 0011101101101:3 0011101101111:12 0011101110101:9
0011101110111:7 0011101111011:3 0011101111101:7 0011101111111:5
0011110011111:7 0011110101011:8 0011110101101:8 0011110101111:8
0011110110101:11 0011110110111:11 0011110111011:8 0011110111101:6
0011110111111:8 0011111010101:7 0011111010111:7 0011111011011:12
0011111011101:9 0011111011111:5 0011111101011:12 0011111101101:5
0011111101111:12 0011111110101:7 0011111110111:7 0011111111011:1
0011111111101:9 0011111111111:5 0101010101011:6 0101010101111:4
0101010110111:2 0101010111011:4 0101010111111:4 0101011010111:0
0101011011011:2 0101011011111:2 0101011101011:6 0101011101111:6
0101011110111:2 0101011111011:4 0101011111111:4 0101101011011:9
0101101011111:11 0101101101111:2 0101101110111:11 0101101111011:2
0101101111111:0 0101110101111:4 0101110110111:0 0101110111011:4
0101110111111:4 0101111011011:4 0101111011111:0 0101111101111:6
0101111110111:0 0101111111011:4 0101111111111:2 0110110110111:11
0110110111111:10 0110111011111:7 0110111101111:10 0110111110111:7
0110111111111:7 0111011101111:4 0111011111111:4 0111101111111:9
0111110111111:4 0111111111111:0
```

References

[1] A. Alhakim and M. Akinwande, *A recursive construction of nonbinary de Bruijn sequences*, Des. Codes Cryptogr. **60** (2011), no. 2, 155–169.

[2] T. van Aardenne-Ehrenfest and N. G. de Bruijn, *Circuits and trees in oriented linear graphs*, Simon Stevin **28** (1951), 203–217.

[3] D. A. Cartwright, M. A. Cueto, and E. A. Tobis, *The maximum independent sets of de Bruijn graphs of diameter 3*, Electron. J. Combin. **18** (2011), no. 1, Paper P194.
[4] D.-Z. Du, F. Cao, and D. F. Hsu, *De Bruijn digraphs, Kautz digraphs, and their generalizations*, in *Combinatorial Network Theory*, Kluwer Acad. Publ., Dordrecht, 1996, pp. 65–105.
[5] N. G. de Bruijn, *A combinatorial problem*, Proc. Kon. Ned. Akad. Wetensch. **49** (1946), 758–764.
[6] T. Etzion, *Sequences and the de Bruijn Graph: Properties, Constructions, and Applications*, Academic Press, London, 2024.
[7] H. Fredricksen and J. Maiorana, *Necklaces of beads in k colors and k-ary de Bruijn sequences*, Discrete Math. **23** (1978), no. 3, 207–210.
[8] H. Fredricksen, *A survey of full length nonlinear shift register cycle algorithms*, SIAM Rev. **24** (1982), no. 2, 195–221.
[9] N. Lichiardopol, *Independence number of de Bruijn graphs*, Discrete Math. **306** (2006), no. 12, 1145–1160.
[10] P. Majer and M. Novaga, *Monotone paths in random hypergraphs*, Electron. J. Combin. **19** (2012), no. 2, Paper 17.
[11] A. Ralston, *De Bruijn sequences—a model example of the interaction of discrete mathematics and computer science*, Math. Mag. **55** (1982), no. 3, 131–143.
[12] W. T. Trotter and P. Winkler, *Ramsey theory and sequences of random variables*, Combin. Probab. Comput. **7** (1998), no. 2, 221–238.

Dipartimento di Matematica, Università di Pisa, Largo Bruno Pontecorvo 5, 56127 Pisa, Italy
Email address: pietro.majer@unipi.it

Dipartimento di Matematica, Università di Pisa, Largo Bruno Pontecorvo 5, 56127 Pisa, Italy
Email address: matteo.novaga@unipi.it