Equitable orientations of sparse uniform hypergraphs
Nathann Cohen, William Lochet

To cite this version:

HAL Id: hal-01417832
https://hal.archives-ouvertes.fr/hal-01417832
Submitted on 16 Dec 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers. L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Equitable orientations of sparse uniform hypergraphs

Nathann Cohen
CNRS and Université Paris-Sud
nathann.cohen@gmail.com

William Lochet*
Université Côte d’Azur, CNRS, Inria, I3S, France
LIP, ENS de Lyon, CNRS, Université de Lyon, France
william.lochet@gmail.com

Submitted: May 20, 2016; Accepted: Jan 2, 2012; Published: XX
Mathematics Subject Classifications: 05C65, 05D40

Abstract

Caro, West, and Yuster studied how \( r \)-uniform hypergraphs can be oriented in such a way that (generalizations of) indegree and outdegree are as close to each other as can be hoped. They conjectured an existence result of such orientations for sparse hypergraphs, of which we present a proof.

1 Introduction

In [1], Caro, West, and Yuster presented a generalization to hypergraphs of the notion of orientation defined for graphs. Their acknowledged purpose is to study how hypergraphs can be oriented in such a way that minimum and maximum degree are close to each other, knowing that reaching an additive difference of \( \leq 1 \) is always achievable in the case of graphs. Identifying an orientation of an edge with a total ordering of its elements, they define a notion of degree on oriented \( r \)-uniform hypergraphs.

**Definition 1.** Let \( \mathcal{H} \) be a \( r \)-uniform hypergraph, and let every \( S \in \mathcal{H} \) define a total order on its elements as a bijection \( \sigma_S : S \mapsto [r] \). The degree \( d_P(U) \) of a set of vertices \( U \subseteq V(\mathcal{H}) \) with respect to a set of positions \( P \subseteq [r] \) (where \( |U| = |P| \)) is equal to:

\[
d_P(U) = |\{ S \in \mathcal{H} : U \subseteq S \text{ and } \sigma_S(U) = P \}|
\]

From there they define equitable orientations:

**Definition 2.** The orientation of a \( r \)-uniform hypergraph \( \mathcal{H} \) is said to be \( p \)-equitable if \( |d_P(U) - d_{P'}(U)| \leq 1 \) for any choice of \( U \subseteq V(\mathcal{H}) \) and \( P, P' \subseteq [r] \) of cardinality \( p \). It is said to be nearly \( p \)-equitable if the looser requirement \( |d_P(U) - d_{P'}(U)| \leq 2 \) holds.

*Supported by ANR under contract STINT ANR-13-BS02-0007*
They gave proof that all hypergraphs admit a 1-equitable as well as a \((r - 1)\)-equitable orientation, and also proved that some hypergraphs do not admit a \(p\)-equitable orientation for all values of \(p\). Additionally, they parameterized the notion of maximum degree in order to focus on hypergraphs which are \textit{sparse} with respect to the problem at hand:

\[
\Delta_p(\mathcal{H}) = \max_{U \subseteq V(\mathcal{H})} \left| \{ S \in \mathcal{H} : U \subseteq S \} \right|
\]

Thus, they proved that for any fixed value of \(p\) and \(k\), and for every sufficiently large integer \(r\), every \(r\)-uniform hypergraph \(\mathcal{H}\) with \(\Delta_p(\mathcal{H}) \leq k\) admits a nearly \(p\)-equitable orientation. They conjectured that this setting actually ensured the existence of a \(p\)-equitable orientation, which we prove here.

**Theorem 3.** Let \(p, k\) be fixed integers. There exists \(r_0\) such that for every \(r \geq r_0\), every \(r\)-uniform hypergraph with \(\Delta_p(\mathcal{H}) \leq k\) admits a \(p\)-equitable orientation.

Note that, as \(r\) is big compared to \(\Delta_p(\mathcal{H})\), a \(p\)-equitable orientation means that \(d_P(U)\) is equal to 0 or 1 for every choice of set of positions \(P\) and set of vertices \(U\).

In order to prove the existence of nearly \(p\)-equitable orientation, Caro, West, and Yuster [1] used the Lovász Local Lemma. In [3], Moser and Tardos presented an elegant algorithmic proof of it which developed the technique of entropy compression. Our proof uses that technique and the following Lemma (proved in Section 3) that counts what can be seen as a generalization of derangements.

**Lemma 4.** Let \(p, k \in \mathbb{N}\) and \(\alpha < 1\) be fixed. Let \(X\) be a set of cardinality \(r\) and let \(L_S\) be, for every \(S \in \binom{X}{p}\), a collection of \(p\)-subsets of \(X\) with \(|L_S| \leq k\). Then, if no \(p\)-subset occurs in more than \(r^\alpha\) of the \(L_S\), a random permutation \(\sigma\) of \(X\) satisfies \(\sigma(S) \notin L_S\) for every \(S\) with probability \(\geq \left(1 - 2k/\binom{r}{p}\right)^\binom{r}{p} = e^{-2k} + o(1)\) when \(r\) grows large.

## 2 Algorithm

In what follows, we assume that every finite set \(S\) has an implicit enumeration on its elements, and in particular that the edges of a hypergraph \(\mathcal{H}\) are implicitly ordered. We will say that \(i\) \textit{represents} an element \(s \in S\) when \(s\) is the \(i\)-th element of \(S\) in this implicit ordering.

We will orient the edges of \(\mathcal{H}\) one by one as a (partial) equitable orientation of \(\mathcal{H}\), i.e. in such a way that any \(p\)-subset of \(V(\mathcal{H})\) never appears more than once at the same position among the oriented edges. To do so, we require the partial orientation to enforce an additional property.

**Definition 5.** Let \(\mathcal{H}\) be a partially oriented \(r\)-uniform hypergraph. We say that an edge \(S \in \mathcal{H}\) is \textit{pressured} by a family \(\{S_1, \ldots, S_l\}\) of edges (oriented by \(\sigma_{S_1}, \ldots, \sigma_{S_l}\)) if there exists \(P \in \binom{[r]}{p}\) such that \(\sigma_{S_i}^{-1}(P) \subseteq S\) for every \(i\).
Note that Lemma 11 ensures that a partial orientation of $\mathcal{H}$ can be extended to an unoriented edge $S$, provided that no family of more than $r^\alpha$ oriented edges pressures $S$. It asserts, for $c < e^{-2k}$ and $r$ sufficiently large, that at least $cr!$ orientations of $S$ are admissible for this extension: we name them good permutations of $S$. Algorithm 1 selects an ordering randomly among them, while ensuring that no other edge is pressured by a family of edges larger than $r_1 = \lceil r^\alpha \rceil$.

**Data:** A $r$-uniform hypergraph $\mathcal{H}$ with $\Delta_p(\mathcal{H}) \leq k$

**Result:** A $p$-equitable orientation of $\mathcal{H}$

**Algorithm 1:** A non-deterministic algorithm

Algorithm 1 starts with every edge being unoriented. At each step it orients the unoriented edge of smallest index by choosing a random permutation amongst the $cr!$ first good permutations. We call bad event the event that an edge $S \in \mathcal{H}$ is pressured by a family $\{S_1, \ldots, S_r\}$ of cardinality $r_1$. If a bad event occurs after orienting $S_1$, then the algorithm erases the orientation of the $S_1, \ldots, S_{r_1}$.

It is trivial to see that Algorithm 1 only returns $p$-equitable orientations of $\mathcal{H}$. Moreover, every time the algorithm chooses a random permutation, it does so among at least $cr!$ good ones by Lemma 11. Note that we need to consider large families pressuring already oriented edges: indeed, we might have to cancel the orientation of such an edge to redefine it again later.

**Theorem 6.** Let $p, k \in \mathbb{N}$, $\alpha, c \in \mathbb{R}_{>0}$ with $\alpha < 1$ and $c < e^{-2k}$. For every sufficiently large $r$, there is a set of random choices for which Algorithm 1 terminates.

In order to prove this result we will analyse the possible executions of the $M$ first steps of Algorithm 1. To this end we make it deterministic by defining a log (following the idea of [3]) and obtain Algorithm 2, in the following way:

- Take as input a vector $v \in [cr!]^M$ which simulates the random choices.
- Output a log when it is not able to orient all edges.

We define a log of order $M$ to be a triple $(R, X, F)$ where:

- $R$ is a binary word whose length lies between $M$ and $2M$.
- $X$ is a sequence of $h$ 7-tuples of integers $(x_1, x_2, x_3, x_4, x_5, x_6, x_7)$ where:
\begin{align*}
x_1 & \leq {r \choose p} \\
x_2 & \leq k \\
x_3 & \leq \binom{r}{r_1-1} \\
x_4 & \leq k^{r_1-1} \\
x_5 & \leq p^{r_1-1} \\
x_6 & \leq (r-p)^{r_1-1} \\
x_7 & \leq r!
\end{align*}

- \( F \) is an integer smaller than \((r! + 1)^{|\mathcal{H}|}\) representing a partial orientation of \( \mathcal{H} \).

The log of order \( M \) (or just log) is actually a trace of the deterministic algorithm’s execution after \( M \) steps. Its objective is to encode which orientations get canceled during the algorithm’s execution. We will show later that Algorithm 2 cannot produce the same log from two different input vectors \( v, v' \in [cr!]^M \) and that, for \( M \) big enough, that the set of possible log is smaller than \((cr!)^M\). We now describe the log and how Algorithm 2 produces it.

- \( R \) is initialized to the empty word. We append 1 to \( R \) whenever Algorithm 2 adds a new orientation; we append 0 whenever it cancels one.

- Consider the following bad event: after orienting \( S_1 \), an edge \( S \in \mathcal{H} \) is pressured by a family \( \{S_1, \ldots, S_{r_1}\} \) of cardinality \( r_1 \). We note \( s_i \) the set of vertices that \( S_i \) maps to \( P \). We associate the following 7-tuple which identifies the sets \( S_i \) as well as their orientation:
  - \( x_1 < \binom{r}{p} \) represents the set \( s_1 \) among the \( \binom{r}{p} \) possible subsets of size \( p \) of \( S_1 \).
  - \( x_2 < k \) identifies \( S \) as one of the (at most \( k \)) edges containing \( s_1 \).
  - \( x_3 < \binom{r}{r_1-1} \) is an integer representing the set of subsets \( s_2, \ldots s_{r_1} \) amongst the \( \binom{r}{p} \) subsets of size \( p \) of \( S \).
  - \( x_4 < k^{r_1-1} \) is an integer representing the sequence \((y_2, \ldots, y_{r_1}) \in [k]^{r_1-1}\) such that the \( y_l \)-th edge containing \( s_l \) is \( S_l \).
  - \( x_5 < p^{r_1-1} \) is an integer representing the sequence \((p_1, \ldots, p_{r_1})\), where \( p_i \in [p!] \) represents the subpermutation of \( S_i \) onto \( s_i \) (we know it’s a permutation of \( P \)).
  - \( x_6 < (r-p)^{r_1-1} \) is the integer representing the sequence \([p_2, \ldots, p_{r_1}]\), where \( p_i \in [(r-p)!] \) represent the subpermutation of \( S_i \) onto \([r] \setminus s_i \).
  - \( x_7 < r! \) is the integer representing the permutation chosen for \( S_1 \).

\( X \) is the list of the 7-tuples describing the bad events, in the order in which they happen.

- \( F \) is the integer representing the partial orientation of \( \mathcal{H} \) (i.e. a choice among \( r! + 1 \) per edge of \( \mathcal{H} \)) after \( M \) steps.
This gives the following Algorithm 2:

**Data:**
1. A \( r \)-uniform hypergraph \( \mathcal{H} \) with \( \Delta_p(\mathcal{H}) \leq k \),
2. A vector \( v \in [cr!]^M \)

**Result:** A \( p \)-equitable orientation of \( \mathcal{H} \), or a log of order \( M \)

\[
R \leftarrow \emptyset, X \leftarrow \emptyset
\]

**for** \( 1 \leq i \leq M \) **do**

\[
S_1 \leftarrow \text{unoriented edge of smallest index}
\]

**if** some edge of \( \mathcal{H} \) is pressured by \( \{S_1, \ldots, S_{r_1}\} \) **then**

\[
\begin{align*}
&\text{Append 1 to the end of } R \\
&\text{Append to } X \text{ a 7-tuple describing the conflict} \\
&\text{Cancel the orientation of all } r_1 + 1 \text{ edges involved in the conflict}
\end{align*}
\]

**else if** all edges are oriented **then**

\[
\text{Return the oriented } \mathcal{H}
\]

**else**

\[
\text{Append 0 to the end of } R
\]

**end**

\[
F \leftarrow \text{the integer representing the partial orientation of } \mathcal{H}.
\]

**Return** \((R, X, F)\)

**Algorithm 2:** A deterministic algorithm

We will show the following claim.

**Claim 7.** Let \( e \) be a vector in \([cr!]^M\) from which Algorithm 2 cannot produce a \( p \)-equitable orientation of \( \mathcal{H} \) and outputs a log \((R, X, F)\). We can reconstruct \( e \) from \((R, X, F)\).

**Proof of the claim.** First we show that we can find, for every \( z \leq M \), the set \( C(z) \) of edges which are oriented after \( z \) steps. We proceed by induction on \( z \), starting from \( C(0) = \emptyset \).

At step \( z + 1 \), Algorithm 2 chooses a orientation for the smallest index \( i \) not in \( C(z) \). If, in \( R \), the \( (z + 1)\)-th 1 is not followed by a 0, then there is no bad event triggered by this step. In this case the set \( C(z + 1) \) is the set \( C(z) \cup i \). Suppose now that the \( (z + 1)\)-th 1 is followed by a sequence of 0: this means that the algorithm encountered a bad event. By looking at the number of sequences of 0 in \( R \) before the \( z + 1\)-th 1 we can deduce the number of bad events before this one. This mean we can find, in \( X \), the 7-tuple \((x_1, x_2, x_3, x_4, x_5, x_6, x_7)\) associated to this bad event. We take the following notations for the bad event: After orienting \( S_1 \), an edge \( S \) of \( \mathcal{H} \) is pressured by a family \( \{S_1, \ldots, S_{r_1}\} \) of cardinality \( r_1 \). We note \( s_t \) the subset of \( S_t \) that are sent to \( P \). \( S_1 \) is the last edge we oriented (known by induction), \( x_1 \) indicates \( s_1 \) amongst the subset of \( S \), \( x_2 \) indicates \( S \) amongst the set of edges containing \( s_1 \), \( x_3 \) indicates the \( s_d \) for \( d \in [2..r_1] \), and \( x_4 \) indicates the \( S_d \) for \( d \in [2..r_1] \). In this case the set \( C(z + 1) \) is the set \( C(z) \) for which we removed all the \( ES_d \) for \( d \in [2..r_1] \).
We can now deduce the set $S(z)$ of all chosen orientations after $z$ steps. We also proceed by induction, this time starting from step $M$. By construction, $F$ is exactly the integer representing the partial orientation of $H$ at step $M$. If the last letter of $R$ is a 1, this means the last step of the algorithm consisted only of choice of an orientation. We just showed that we know which orientation was chosen after $M-1$ steps, so we can deduce the state of all orientation after $M-1$ steps. If the last letter is a 0, Algorithm 2 encountered a bad event. Keeping the notation of the bad event, let $(M)$ be the 7-tuple associated to this bad event. Like before $x_1$, $x_2$, $x_3$, $x_4$ and the knowledge of $C(M-1)$ allow us to know which permutations Algorithm 2 erased at this step. Moreover $x_7$ tells us the random choice made by Algorithm 2 and from $x_7$ and $x_1$ we can deduce $P$. For each $s_i$ we know the orientation chosen for $x_i$ at the step $M-1$ sends $P$ onto $s_i$, from $x_5$ we deduce exactly in which order and from $x_6$ we get the rest of the orientation. Therefore we can deduce the set of chosen orientations before the bad event occurred. With the sets $S(z)$ and $C(z)$ known for all $z \leq M$ we can easily deduce $e$.

The previous claim has the following corollary:

**Corollary 8.** If $H$ admits no $p$-equitable orientation, then Algorithm 2 defines an injection from the set of vectors $(c r!)^M$ into $L^M$.

Let $L_M$ be the set of all possible logs after $M$ steps of Algorithm 2. To show Theorem 6 it suffices to show that, for $M$ big enough, $|L_M|$ is strictly smaller than $(c r!)^M$.

**Lemma 9.** For $M$ big enough, $|L_M| < (c r!)^M$.

**Proof.** We will compute a bound for $|L_M|$. $R$ is a binary word of size $\leq 2M$, and there are at most $4^M$ such words. $X$ is a list of 7-tuples. As Algorithm 2 made $M$ choices and each bad event removes $r_1$ of those, there exist at most $\frac{M}{r_1}$ bad events. Moreover, for each 7-tuple, $(x_1, x_2, x_3, x_4, x_5, x_6, x_7)$ we have $x_1 \leq \left(\begin{array}{c} p \\ r_1-1 \end{array}\right)$, $x_2 \leq k$, $x_3 \leq \left(\begin{array}{c} p \\ r_1-1 \end{array}\right)$, $x_4 \leq k^{r_1-1}$, $x_5 \leq p^{r_1-1}$, $x_6 \leq (r-p)!^{r_1-1}$, $x_7 \leq r!$. Using the bounds $\left(\begin{array}{c} p \\ r_1 \end{array}\right) \leq \frac{n^p}{r_1^p}$ or $\left(\begin{array}{c} p \\ k \end{array}\right) \leq n^k$ we get the following bound.

$$
|X| \leq \left( p^p \cdot k \cdot \left( \begin{array}{c} p^p \cdot e \\ r_1-1 \end{array}\right) \right)^{r_1-1} \cdot \left( k \cdot p! \cdot (r-p)!^{r_1-1}\right) \cdot r!
$$

$$
\leq \left( \frac{(r! \cdot (r^p) r_1 \cdot (r-p)!^{r_1-1})^{M/r_1}}{(r_1-1)^{M(r_1-1)/r_1}} \cdot (k \cdot e \cdot p!)^M \right)
$$

$$
\leq \left[ p^p \cdot r! r_1^p \cdot \left( \frac{r^p}{(r_1-1)(r_1-1)/r_1} \right)^{r_1-1} \cdot \left( \frac{k \cdot e \cdot p!}{(r_1-1)(r_1-1)/r_1} \right)^M \right]
$$

We can assume $r > 2p$, and so $\frac{r}{r-p+1} < 2$:

$$
|X| \leq r!^M \cdot \left( p^p/r_1 \cdot 2p \cdot \frac{k \cdot e \cdot p!}{(r_1-1)(r_1-1)/r_1} \right)^M
$$
As $|F| \leq (r! + 1)^{|H|}$ and $|L_M| \leq |F||X||R|$ we get the following bound on $|L_M|:

$$|L_M| \leq r!M \cdot \left(4 \cdot r^{p/r_1} \cdot 2^p \cdot \frac{k \cdot e \cdot p!}{(r_1 - 1)^{(r_1-1)/(r_1)}}\right)^M \cdot (r! + 1)^{|H|}$$

\[\square\]

3 Derangements

The results of this section are based on a lemma from Erdős and Spencer [2]:

**Lemma 10** (LopsidedLovász Local Lemma). Let $A_1, \ldots, A_m$ be events in a probability space, each with probability at most $p$. Let $G$ be a graph defined on those events such that for every $A_i$, and for every set $S$ avoiding both $A_i$ and its neighbours, the following relation holds:

$$P[A_i \bigcap \bigcap_{A_j \in S} \bar{A}_j] \leq P[A_i]$$

Then if $4dp \leq 1$, all the events can be avoided simultaneously:

$$P[\bar{A}_1 \land \cdots \land \bar{A}_m] \geq (1 - 2p)^m > 0$$

Thanks to this result we can prove the following, which can be seen as a generalization of the fact that a random permutation of $n$ points is a derangement with asymptotic probability $1/e$.

**Lemma 11.** Let $p, k \in \mathbb{N}$ and $\alpha < 1$ be fixed. Let $X$ be a set of cardinality $r$ and let $L_S$ be, for every $S \in \binom{X}{p}$, a collection of $p$-subsets of $X$ with $|L_S| \leq k$. Then, if no $p$-subset occurs in more than $r^\alpha$ of the $L_S$, a random permutation $\sigma$ of $X$ satisfies $\sigma(S) \notin L_S$ for every $S$ with probability $\geq (1 - 2k/\binom{r}{p})^{\binom{r}{p}} = e^{-2k} + o(1)$ when $r$ grows large.

**Proof.** For every $S \in \binom{X}{p}$, we define the bad event $B_S$ with:

$$B_S = \bigvee_{S' \in L_S} [\sigma(S) = S']$$

Each $B_S$ has a probability $P[B_S] \leq k/\binom{r}{p}$. On these bad events we define a lopsidependency graph (see [2]) $G_B$ with the following adjacencies:

$$\left\{(B_{S_1}, B_{S_2}) : S_1, S_2 \in \binom{X}{p} \text{ s.t. } \left[ S_1 \cup L_{S_1} \right] \cap \left[ S_2 \cup L_{S_2} \right] \neq \emptyset \right\}$$

As a $p$-subset of $X$ intersects at most $O(r^{p-1})$ others, and noting that every $p$-subset can occur at most $r^\alpha$ times, we have that:

$$\Delta(G_B) \leq (k + 1)r^\alpha \times O(r^{p-1}) = o(r^p)$$
In order to apply the Lopsided Lovász Local Lemma to the events $B_S$ and graph $G_B$, we must ensure for every $S \subseteq \binom{X}{p}$ and $S_B \subseteq V(G_B) \setminus N_{G_B}[B_S]$ that:

$$P(B_S \mid \bigwedge_{B_{S'} \in S_B} \bar{B}_{S'}) \leq P(B_S)$$  \hspace{1cm} (1)

Indeed, if we denote by $T$ (for trace) the number of elements of $\bigcup_{B_{S'} \in S_B} S'$ sent by the random permutation $\sigma$ into $\bigcup L_S$:

$$P(B_S) = \sum_t P(B_S \mid T = t)P(T = t)$$

$$P(B_S \mid \bigwedge_{B_{S'} \in S_B} \bar{B}_{S'}) = \sum_t P(B_S \mid T = t, \bigwedge_{B_{S'} \in S_B} \bar{B}_{S'})P(T = t \mid \bigwedge_{B_{S'} \in S_B} \bar{B}_{S'})$$

As $\bigcup L_S$ is disjoint from the $\bigcup L_{S'}$, $\forall B_{S'} \in S_B$, we have:

$$P(B_S \mid T = t, \bigwedge_{B_{S'} \in S_B} \bar{B}_{S'}) = P(B_S \mid T = t)$$

And thus:

$$P(B_S \mid \bigwedge_{B_{S'} \in S_B} \bar{B}_{S'}) = \sum_t P(B_S \mid T = t)P(T = t \mid \bigwedge_{B_{S'} \in S_B} \bar{B}_{S'})$$

In order to prove (1), we will first need the following observation:

**Claim 12.** $P(B_S \mid T = t)$ is a decreasing function of $t$.

**Proof of the claim.** We compute the value of $P(B_S \mid T = t)$ exactly, denoting by $r' \leq r$ the cardinality of $\bigcup_{B_{S'} \in S_B} S'$. It is equal to 0 when $t > r' - p$, and is otherwise equal to:

$$P(B_S \mid T = t) = \sum_{S' \in L_S} P(\sigma(S) = S' \mid T = t)$$

$$= \frac{|L_S|(r' - p)}{r!} \binom{r'}{t} \binom{r'}{t'} \binom{(r - p - t)!}{r'} \binom{(r' - t)!}{r - t}$$

$$= P(B_S \mid T = t - 1) \left( \frac{(r' - p - t + 1)(r - t + 1)}{(r - p - t + 1)(r' - t + 1)} \right)$$

$$\leq P(B_S \mid T = t - 1)$$

Additionally, we will prove a relationship on the members of $\sum_t P(T = t)$ and on those of $\sum_t P(T = t \mid \bigwedge_{B_{S'} \in S_B} \bar{B}_{S'})$, which both sum to 1.
Claim 13. If \( P(T = t \mid \bigwedge_{B_{S'} \in S_B} \bar{B}_{S'}) \) is nonzero, then
\[
\frac{P(T = t + 1)}{P(T = t)} \leq \frac{P(T = t + 1 \mid \bigwedge_{B_{S'} \in S_B} \bar{B}_{S'})}{P(T = t \mid \bigwedge_{B_{S'} \in S_B} \bar{B}_{S'})}
\]

Proof of the claim. According to Bayes’ Theorem applied to the right side of the equation,
\[
\frac{P(T = t + 1 \mid \bigwedge_{B_{S'} \in S_B} \bar{B}_{S'})}{P(T = t \mid \bigwedge_{B_{S'} \in S_B} \bar{B}_{S'})} = \frac{P(\bigwedge_{B_{S'} \in S_B} \bar{B}_{S'} \mid T = t + 1) P(T = t + 1)}{P(\bigwedge_{B_{S'} \in S_B} \bar{B}_{S'} \mid T = t) P(T = t)}
\]
We thus only need to ensure the following, which is a consequence of Lemma 14:
\[
P(\bigwedge_{B_{S'} \in S_B} \bar{B}_{S'} \mid T = t + 1) \geq P(\bigwedge_{B_{S'} \in S_B} \bar{B}_{S'} \mid T = t)
\]
\(\diamondsuit\)

We are now ready to prove (1), and we define \( d_t \) for every \( t \) where \( P(T = t) \) is nonzero:
\[
d_t = P(T = t) - P(T = t \mid \bigwedge_{B_{S'} \in S_B} \bar{B}_{S'})
\]
Because \( d_t \) is a difference of probability distributions the sum \( \sum_t d_t \) is null, and we can rewrite (1) using \( d_t \):
\[
0 \leq P(B_S) - P(B_S \mid \bigwedge_{B_{S'} \in S_B} \bar{B}_{S'}) \\
\leq \sum_t P(B_S \mid T = t) P(T = t) - \sum_t P(B_S \mid T = t) P(T = t \mid \bigwedge_{B_{S'} \in S_B} \bar{B}_{S'}) \\
\leq \sum_t d_t P(B_S \mid T = t)
\]
We will thus prove that the sum \( \sum_t d_t P(B_S \mid T = t) \) is nonnegative. It is a consequence of Claim 13 that all nonnegative values of \( d_t \) appear before all nonpositive ones, and so that there is a \( t_0 \) such that \( d_t \geq 0 \) iff \( t \leq t_0 \). As a result, \( |\sum_{t \leq t_0} d_t| = |\sum_{t > t_0} d_t| = \frac{1}{2} \) and we can write:
\[
\sum_t d_t P(B_S \mid T = t) = \sum_{t \leq t_0} d_t P(B_S \mid T = t) + \sum_{t > t_0} d_t P(B_S \mid T = t) \\
\geq \frac{1}{2} P(B_S \mid T = t_0) - \frac{1}{2} P(B_S \mid T = t_0 + 1) \geq 0 \quad \text{(by Claim 12)}
\]
The second hypothesis of Lemma 10 is that \( 4pd \ll 1 \), which translates in our case to \( 4\frac{k}{(p)} o(r^p) = o(1) \) and is thus satisfied when \( r \) grows large. Hence, we have that:
\[
P(\bigwedge_{B_S} \bar{B}_S) \geq \left[ 1 - 2k/\binom{r}{p} \right]^{(r)} = e^{-2k} + o(1)
\]
\(\square\)
Lemma 14. Let $A, B$ be two sets of size $r$, and let $\sigma : A \mapsto B$ be a random bijection. For every $A_1, \ldots, A_k \subseteq A \subseteq A'$ and $B_1, \ldots, B_k \subseteq B' \subseteq B$, the following function increases with $t$.

\[ P \left[ \bigwedge_i [\sigma(A_i) \neq B_i] \mid \sigma(A') \setminus B' \text{ has cardinality } t \right] \tag{2} \]

Proof. We implicitly assume in this proof that the conditioning event has a nonzero probability for $t$ and $t+1$. Let $S_1, S_2$ be two sets of cardinality $|A'|$ with symmetric difference $S_1 \Delta S_2 = \{x, y\}$ where $x \in S_2$ is an element of $B \setminus B'$. Let $\sigma_{xy}$ be the permutation transposing $x$ and $y$. Then,

\[
P \left[ \bigwedge_i [\sigma(A_i) \neq B_i] \mid \sigma(A') = S_1 \right] \leq P \left[ \bigwedge_i [\sigma_{xy}\sigma(A_i) \neq B_i] \mid \sigma(A') = S_1 \right] = P \left[ \bigwedge_i [\sigma(A_i) \neq B_i] \mid \sigma(A') = S_2 \right] \]

We are now ready to derive the result:

\[
(2) = \frac{1}{\binom{|B|}{t} \binom{|A'|}{t}} \sum_{2 \leq \beta \leq \gamma} \frac{1}{\binom{|B \setminus B'|}{t} + 1} \sum_{\beta \subseteq \gamma} P \left[ \bigwedge_i [\sigma(A_i) \neq B_i] \mid \sigma(A') = \delta \right] \]

Using our previous remark, we find an upper bound on the last term of the equation by averaging it over sets $S'$ obtained from $S$ by the exchange of two elements:

\[
(2) \leq \frac{1}{\binom{|B|}{t} \binom{|A'|}{t}} \sum_{2 \leq \beta \leq \gamma} \frac{1}{\binom{|B \setminus B'|}{t} + 1} \sum_{\beta \subseteq \gamma} P \left[ \bigwedge_i [\sigma(A_i) \neq B_i] \mid \sigma(A') = \delta \right] = \frac{1}{\binom{|B|}{t} \binom{|A'|}{t}} \sum_{2 \leq \beta \leq \gamma} \frac{1}{\binom{|B \setminus B'|}{t} + 1} \sum_{\beta \subseteq \gamma} P \left[ \bigwedge_i [\sigma(A_i) \neq B_i] \mid \sigma(A') = S' \right] = \frac{1}{\binom{|B|}{t} \binom{|A'|}{t}} \sum_{2 \leq \beta \leq \gamma} \frac{1}{\binom{|B \setminus B'|}{t} + 1} \sum_{\beta \subseteq \gamma} P \left[ \bigwedge_i [\sigma(A_i) \neq B_i] \mid \sigma(A') \setminus B' \text{ has cardinality } t + 1 \right] \]

\[
P \left[ \bigwedge_i [\sigma(A_i) \neq B_i] \mid \sigma(A') \setminus B' \text{ has cardinality } t + 1 \right] \]

References
