PCP теорема. Часть 2

М. Вялый

МФТИ, 19.03.2013

Задача k-выполнимости

Гиперграф ограничений $G(V, E, \Sigma, c)$

- V — вершины графа (переменные)
- E — мультимножество ребер, каждое ребро $e \in V^k$
- Σ — алфавит (конечное множество)
- c — ограничения. Для каждого ребра $e \in E$ указано $c_e \subseteq \Sigma^k$.

Присваивания, выполнение ограничений, потери

- Присваивание: $\sigma\colon V \to \Sigma$
- Ограничение c_e, $e = (v_1, \dots, v_k)$, выполнено, если
$$(\sigma(v_1), \dots, \sigma(v_k)) \in c_e \subseteq \Sigma^k$$
- Потери на присваивании $\mathrm{UNSAT}_\sigma(G)$ — доля ограничений, не выполненных на σ
- Потери в задаче $\mathrm{UNSAT}(G) = \min_\sigma \mathrm{UNSAT}_\sigma(G)$

Общая схема доказательства PCP теоремы

1. $O(\log n)$ раз применяется «сводимость удвоения зазора» между задачами 2-выполнимости
$$G(V, E, \Sigma, c) \mapsto G'(V', E', \Sigma, c'),$$
которая
2. увеличивает зазор в два раза $\mathrm{UNSAT}(G') \geqslant \max(2\mathrm{UNSAT}(G), \alpha)$, $\alpha = \Omega(1)$,
3. размер задачи изменяет линейно,
4. алфавит не меняет.

«Сводимость удвоения зазора» состоит в композиции четырех преобразований

1. Улучшение графа ограничений.
2. Увеличение зазора за счет увеличения алфавита.
3. Уменьшение алфавита за счет увеличения арности.
4. Возврат к 2-выполнимости.

План дальнейшего рассказа

1. Увеличение зазора
2. Уменьшение алфавита: локально проверяемые коды
3. Преобразование k-выполнимости в 2-выполнимость
4. Улучшение графа
5. Выбор параметров

Увеличение зазора

Дано:

Граф ограничений $G(V, E, \Sigma, c)$. Степени вершин d (константа), граф является алгебраическим экспандером с $\lambda(G)/d \leqslant \lambda < 1$ (λ тоже константа). В каждой вершине половина ребер — петли.

Построить:

Граф ограничений $G'(V', E', \Sigma', c')$ такой, что

$$\textsc{unsat}(G) = 0 \quad \Rightarrow \quad \textsc{unsat}(G') = 0,$$

$$\textsc{unsat}(G) \neq 0 \quad \Rightarrow \quad \textsc{unsat}(G') \geqslant \beta\sqrt{t}\min(\textsc{unsat}(G), 1/\sqrt{t}).$$

Здесь β — константа, которая зависит от $|\Sigma|, \lambda, d$, но не зависит от t.

Увеличение зазора

Дано:

Граф ограничений $G(V, E, \Sigma, c)$. Степени вершин d (константа), граф является алгебраическим экспандером с $\lambda(G)/d \leqslant \lambda < 1$ (λ тоже константа). В каждой вершине половина ребер — петли.

Построить:

Граф ограничений $G'(V', E', \Sigma', c')$ такой, что

$$\textsc{unsat}(G) = 0 \quad \Rightarrow \quad \textsc{unsat}(G') = 0,$$

$$\textsc{unsat}(G) \neq 0 \quad \Rightarrow \quad \textsc{unsat}(G') \geqslant \beta\sqrt{t}\min(\textsc{unsat}(G), 1/\sqrt{t}).$$

Здесь β — константа, которая зависит от $|\Sigma|, \lambda, d$, но не зависит от t.

Конструкция графа с увеличенным зазором

- $V' = V$.
- $\Sigma' = \Sigma^{d^{3t}}$ (описание $(3t)$-окрестностей вершин).
  Пусть задана вершина $u \in V$. Тогда компоненту $\vec{\sigma}(u)_v$ символа $\vec{\sigma} \in \Sigma'$ будем называть «мнением u о том, что написано в v».
- E' — маршруты длины $2t + 1$ в G.
- Ограничение в G' на ребре τ (маршруте) с началом в a и концом в b выполнено, если описания окрестностей $\vec{\sigma}(a)$ и $\vec{\sigma}(b)$ согласованы на пересечении окрестностей и выполняются все ограничения на ребрах G, которые попадают в пересечение окрестностей.

Конструкция графа с увеличенным зазором

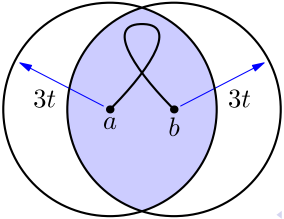
- $V' = V$.
- $\Sigma' = \Sigma^{d^{3t}}$ (описание $(3t)$-окрестностей вершин).
  Пусть задана вершина $u \in V$. Тогда компоненту $\vec{\sigma}(u)_v$ символа $\vec{\sigma} \in \Sigma'$ будем называть «мнением u о том, что написано в v».
- E' — маршруты длины $2t + 1$ в G.
- Ограничение в G' на ребре τ (маршруте) с началом в a и концом в b выполнено, если описания окрестностей $\vec{\sigma}(a)$ и $\vec{\sigma}(b)$ согласованы на пересечении окрестностей и выполняются все ограничения на ребрах G, которые попадают в пересечение окрестностей.

Конструкция графа с увеличенным зазором

- $V' = V$.
- $\Sigma' = \Sigma^{d^{3t}}$ (описание $(3t)$-окрестностей вершин).
  Пусть задана вершина $u \in V$. Тогда компоненту $\vec{\sigma}(u)_v$ символа $\vec{\sigma} \in \Sigma'$ будем называть «мнением u о том, что написано в v».
- E' — маршруты длины $2t+1$ в G.
- Ограничение в G' на ребре τ (маршруте) с началом в a и концом в b выполнено, если описания окрестностей $\vec{\sigma}(a)$ и $\vec{\sigma}(b)$ согласованы на пересечении окрестностей и выполняются все ограничения на ребрах G, которые попадают в пересечение окрестностей.

Конструкция графа с увеличенным зазором

- $V' = V$.
- $\Sigma' = \Sigma^{d^{3t}}$ (описание $(3t)$-окрестностей вершин).
  Пусть задана вершина $u \in V$. Тогда компоненту $\vec{\sigma}(u)_v$ символа $\vec{\sigma} \in \Sigma'$ будем называть «мнением u о том, что написано в v».
- E' — маршруты длины $2t + 1$ в G.
- Ограничение в G' на ребре τ (маршруте) с началом в a и концом в b выполнено, если описания окрестностей $\vec{\sigma}(a)$ и $\vec{\sigma}(b)$ согласованы на пересечении окрестностей и выполняются все ограничения на ребрах G, которые попадают в пересечение окрестностей.



Проверка корректности сводимости

Простая часть:

1. Размер графа изменяется линейно (в предположении, что d и t — константы).
2. Построение G' занимает полиномиальное время от размера G.
3. Если $\mathrm{UNSAT}_\sigma(G) = 0$, то определим $\vec{\sigma}$ как $\vec{\sigma}(u)_v = \sigma(v)$.
4. Тогда на всех ребрах ограничения выполнены: $\mathrm{UNSAT}(G') = 0$.

Трудная часть — оценка увеличения зазора:

- Пусть $\vec{\sigma}$ — оптимальное присваивание в G'. Определим присваивание σ в G подходящим «голосованием» по описаниям соседних вершин.
- Рёбра G, на которых присваивание σ нарушает ограничения, вносят большой вклад в нарушение ограничений в G'. Отсюда получим

$$\mathrm{UNSAT}_{\vec{\sigma}}(G') \geq \beta\sqrt{t}\min(\mathrm{UNSAT}_\sigma(G), 1/\sqrt{t}) \geq \mathrm{UNSAT}(G).$$

Проверка корректности сводимости

Простая часть:

1. Размер графа изменяется линейно (в предположении, что d и t — константы).
2. Построение G' занимает полиномиальное время от размера G.
3. Если $\mathrm{UNSAT}_\sigma(G) = 0$, то определим $\vec\sigma$ как $\vec\sigma(u)_v = \sigma(v)$.
4. Тогда на всех ребрах ограничения выполнены: $\mathrm{UNSAT}(G') = 0$.

Трудная часть — оценка увеличения зазора:

- Пусть $\vec\sigma$ — оптимальное присваивание в G'. Определим присваивание σ в G подходящим «голосованием» по описаниям соседних вершин.
- Рёбра G, на которых присваивание σ нарушает ограничения, вносят большой вклад в нарушение ограничений в $\vec\sigma$. Отсюда получим

$$\mathrm{UNSAT}_{\vec\sigma}(G') \geq \beta\sqrt{t}\min(\mathrm{UNSAT}_\sigma(G), 1/\sqrt{t}) \geq \mathrm{UNSAT}(G).$$

Проверка корректности сводимости

Простая часть:

1. Размер графа изменяется линейно (в предположении, что d и t — константы).
2. Построение G' занимает полиномиальное время от размера G.
3. Если $\mathrm{UNSAT}_\sigma(G) = 0$, то определим $\vec{\sigma}$ как $\vec{\sigma}(u)_v = \sigma(v)$.
4. Тогда на всех ребрах ограничения выполнены: $\mathrm{UNSAT}(G') = 0$.

Трудная часть — оценка увеличения зазора:

- Пусть $\vec{\sigma}$ — оптимальное присваивание в G'. Определим присваивание σ в G подходящим «голосованием» по описаниям соседних вершин.

Проверка корректности сводимости

Простая часть:

1. Размер графа изменяется линейно (в предположении, что d и t — константы).
2. Построение G' занимает полиномиальное время от размера G.
3. Если $\mathrm{UNSAT}_\sigma(G) = 0$, то определим $\vec{\sigma}$ как $\vec{\sigma}(u)_v = \sigma(v)$.
4. Тогда на всех ребрах ограничения выполнены: $\mathrm{UNSAT}(G') = 0$.

Трудная часть — оценка увеличения зазора:

- Пусть $\vec{\sigma}$ — оптимальное присваивание в G'. Определим присваивание σ в G подходящим «голосованием» по описаниям соседних вершин.
- Рёбра G, на которых присваивание σ нарушает ограничения, вносят большой вклад в нарушение ограничений в $\vec{\sigma}$. Отсюда получим

$$\mathrm{UNSAT}_{\vec{\sigma}}(G') \geqslant \beta\sqrt{t}\min(\mathrm{UNSAT}_\sigma(G), 1/\sqrt{t}) \geqslant \mathrm{UNSAT}(G).$$

Проверка корректности сводимости

Простая часть:

1. Размер графа изменяется линейно (в предположении, что d и t — константы).
2. Построение G' занимает полиномиальное время от размера G.
3. Если $\mathrm{UNSAT}_\sigma(G) = 0$, то определим $\vec{\sigma}$ как $\vec{\sigma}(u)_v = \sigma(v)$.
4. Тогда на всех ребрах ограничения выполнены: $\mathrm{UNSAT}(G') = 0$.

Трудная часть — оценка увеличения зазора:

- Пусть $\vec{\sigma}$ — оптимальное присваивание в G'. Определим присваивание σ в G подходящим «голосованием» по описаниям соседних вершин.
- Рёбра G, на которых присваивание σ нарушает ограничения, вносят большой вклад в нарушение ограничений в $\vec{\sigma}$. Отсюда получим

$$\mathrm{UNSAT}_{\vec{\sigma}}(G') \geqslant \beta\sqrt{t}\min(\mathrm{UNSAT}_\sigma(G), 1/\sqrt{t}) \geqslant \mathrm{UNSAT}(G).$$

Проверка корректности сводимости

Простая часть:

1. Размер графа изменяется линейно (в предположении, что d и t — константы).
2. Построение G' занимает полиномиальное время от размера G.
3. Если $\mathrm{UNSAT}_\sigma(G) = 0$, то определим $\vec{\sigma}$ как $\vec{\sigma}(u)_v = \sigma(v)$.
4. Тогда на всех ребрах ограничения выполнены: $\mathrm{UNSAT}(G') = 0$.

Трудная часть — оценка увеличения зазора:

- Пусть $\vec{\sigma}$ — оптимальное присваивание в G'. Определим присваивание σ в G подходящим «голосованием» по описаниям соседних вершин.
- Рёбра G, на которых присваивание σ нарушает ограничения, вносят большой вклад в нарушение ограничений в $\vec{\sigma}$. Отсюда получим

$$\mathrm{UNSAT}_{\vec{\sigma}}(G') \geqslant \beta\sqrt{t}\min(\mathrm{UNSAT}_\sigma(G), 1/\sqrt{t}) \geqslant \mathrm{UNSAT}(G).$$

Голосование

По присваиванию $\vec{\sigma}$ на графе G' строим присваивание σ на G.

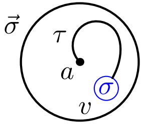
1. На маршрутах длины t с началом в вершине $v \in V$ выбираем равномерное распределение. Пусть $a \in V$ — конец такого случайного маршрута τ.
2. Случайная величина X_v «мнение конца маршрута о том, что написано в его начале».
3. $\sigma(v)$ — значение X_v с наибольшей вероятностью:

$$\sigma(v) = \arg\max_{\sigma\in\Sigma} \mathbf{Pr}[X_v = \sigma].$$

Голосование

По присваиванию $\vec{\sigma}$ на графе G' строим присваивание σ на G.

1. На маршрутах длины t с началом в вершине $v \in V$ выбираем равномерное распределение. Пусть $a \in V$ — конец такого случайного маршрута τ.
2. Случайная величина X_v «мнение конца маршрута о том, что написано в его начале».



$$X_v = \sigma = \vec{\sigma}(a)_v$$

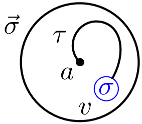
3. $\sigma(v)$ — значение X_v с наибольшей вероятностью:

$$\sigma(v) = \arg\max_{\sigma \in \Sigma} \mathbf{Pr}[X_v = \sigma].$$

Голосование

По присваиванию $\vec{\sigma}$ на графе G' строим присваивание σ на G.

1. На маршрутах длины t с началом в вершине $v \in V$ выбираем равномерное распределение. Пусть $a \in V$ — конец такого случайного маршрута τ.
2. Случайная величина X_v «мнение конца маршрута о том, что написано в его начале».



$$X_v = \sigma = \vec{\sigma}(a)_v$$

3. $\sigma(v)$ — значение X_v с наибольшей вероятностью:

$$\sigma(v) = \arg\max_{\sigma \in \Sigma} \mathbf{Pr}[X_v = \sigma].$$

Анатомия ребер

F — множество «бракованных» ребер, ограничения на которых нарушаются присваиванием σ.

$$\frac{F}{E} = \mathrm{UNSAT}_\sigma(G) < \frac{1}{\sqrt{t}} .$$

Ребро $e = (u, v)$ существенное для маршрута τ с концами a и b, если

$$\vec{\sigma}(a)_u = \sigma(u), \quad \vec{\sigma}(b)_v = \sigma(v)$$

(мнение концов маршрута о концах ребра совпадает с мнением большинства).

Наблюдение

Ограничение на ребре $\tau \in E(G')$ при присваивании $\vec{\sigma}$ нарушается, если на маршруте τ есть хотя бы одно бракованное и существенное ребро.

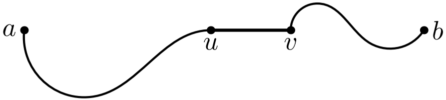
F — множество «бракованных» ребер, ограничения на которых нарушаются присваиванием σ.

$$\frac{F}{E} = \mathrm{UNSAT}_\sigma(G) < \frac{1}{\sqrt{t}}\,.$$

Ребро $e = (u, v)$ существенное для маршрута τ с концами a и b, если

$$\vec{\sigma}(a)_u = \sigma(u), \quad \vec{\sigma}(b)_v = \sigma(v)$$

(мнение концов маршрута о концах ребра совпадает с мнением большинства).



Наблюдение

Ограничение на ребре $\tau \in E(G')$ при присваивании $\vec{\sigma}$ нарушается, если на маршруте τ есть хотя бы одно бракованное и существенное ребро.

Анатомия ребер

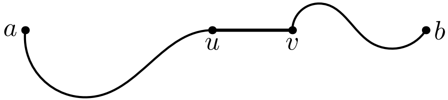
F — множество «бракованных» ребер, ограничения на которых нарушаются присваиванием σ.

$$\frac{F}{E} = \mathrm{UNSAT}_\sigma(G) < \frac{1}{\sqrt{t}}\,.$$

Ребро $e = (u, v)$ существенное для маршрута τ с концами a и b, если

$$\vec{\sigma}(a)_u = \sigma(u), \quad \vec{\sigma}(b)_v = \sigma(v)$$

(мнение концов маршрута о концах ребра совпадает с мнением большинства).



Наблюдение

Ограничение на ребре $\tau \in E(G')$ при присваивании $\vec{\sigma}$ нарушается, если на маршруте τ есть хотя бы одно бракованное и существенное ребро.

$N(\tau)$ — случайная величина, равная количеству бракованных существенных ребер на маршруте τ в его «средней части»: на отрезке между $(t - \delta\sqrt{t})$-м и $(t + \delta\sqrt{t})$-м ребром (δ — еще одна константа).

Тогда из сделанного наблюдения

$$\mathrm{UNSAT}_{\vec{\sigma}}(G') \geqslant \Pr_{\tau \leftarrow U}[N(\tau) > 0]$$

Осталось доказать

$$\Pr_{\tau \leftarrow U}[N(\tau) > 0] > \beta\sqrt{t}\frac{F}{E}.$$

Эта оценка получается из оценок первого и второго моментов $N(\tau)$.

Основная идея оценки

$N(\tau)$ — случайная величина, равная количеству бракованных существенных ребер на маршруте τ в его «средней части»: на отрезке между $(t - \delta\sqrt{t})$-м и $(t + \delta\sqrt{t})$-м ребром (δ — еще одна константа).
Тогда из сделанного наблюдения

$$\mathrm{UNSAT}_{\vec{\sigma}}(G') \geqslant \Pr_{\tau \leftarrow U}[N(\tau) > 0]$$

Осталось доказать

$$\Pr_{\tau \leftarrow U}[N(\tau) > 0] > \beta\sqrt{t}\frac{F}{E}.$$

Эта оценка получается из оценок первого и второго моментов $N(\tau)$.

$N(\tau)$ — случайная величина, равная количеству бракованных существенных ребер на маршруте τ в его «средней части»: на отрезке между $(t - \delta\sqrt{t})$-м и $(t + \delta\sqrt{t})$-м ребром (δ — еще одна константа). Тогда из сделанного наблюдения

$$\mathrm{UNSAT}_{\vec{\sigma}}(G') \geqslant \Pr_{\tau \leftarrow U}[N(\tau) > 0]$$

Осталось доказать

$$\Pr_{\tau \leftarrow U}[N(\tau) > 0] > \beta\sqrt{t}\frac{F}{E}\ .$$

Эта оценка получается из оценок первого и второго моментов $N(\tau)$.

Оценки существенного брака на маршруте

Утверждение (легко проверить)

Если случайная величина X принимает неотрицательные значения, то

$$\mathbf{Pr}[X > 0] \geqslant \frac{(\mathbf{E}(X))^2}{\mathbf{E}(X^2)} .$$

Лемма 1. $\mathbf{E}(N(\tau)) \geqslant \beta' \sqrt{t} \frac{F}{E}$

Лемма 2. $\mathbf{E}(N(\tau)^2) \leqslant \beta'' \sqrt{t} \frac{F}{E}$ при $\frac{F}{E} < \frac{1}{\sqrt{t}}$

Из утверждения и лемм следует требуемое неравенство

$$\mathop{\mathbf{Pr}}_{\tau \leftarrow U}[N(\tau) > 0] > \beta \sqrt{t} \frac{F}{E} .$$

Оценки существенного брака на маршруте

Утверждение (легко проверить)

Если случайная величина X принимает неотрицательные значения, то

$$\mathbf{Pr}[X > 0] \geqslant \frac{(\mathbf{E}(X))^2}{\mathbf{E}(X^2)}\ .$$

Лемма 1. $\mathbf{E}(N(\tau)) \geqslant \beta' \sqrt{t}\frac{F}{E}$

Лемма 2. $\mathbf{E}(N(\tau)^2) \leqslant \beta'' \sqrt{t}\frac{F}{E}$ при $\frac{F}{E} < \frac{1}{\sqrt{t}}$

Из утверждения и лемм следует требуемое неравенство

$$\mathop{\mathbf{Pr}}_{\tau \leftarrow U}[N(\tau) > 0] > \beta\sqrt{t}\frac{F}{E}\ .$$

Оценки существенного брака на маршруте

Утверждение (легко проверить)

Если случайная величина X принимает неотрицательные значения, то

$$\mathbf{Pr}[X > 0] \geqslant \frac{(\mathbf{E}(X))^2}{\mathbf{E}(X^2)} .$$

Лемма 1. $\mathbf{E}(N(\tau)) \geqslant \beta' \sqrt{t}\frac{F}{E}$

Лемма 2. $\mathbf{E}(N(\tau)^2) \leqslant \beta'' \sqrt{t}\frac{F}{E}$ при $\frac{F}{E} < \frac{1}{\sqrt{t}}$

Из утверждения и лемм следует требуемое неравенство

$$\mathbf{Pr}_{\tau \leftarrow U}[N(\tau) > 0] > \beta\sqrt{t}\frac{F}{E} .$$

Оценки существенного брака на маршруте

Утверждение (легко проверить)

Если случайная величина X принимает неотрицательные значения, то

$$\mathbf{Pr}[X > 0] \geqslant \frac{(\mathbf{E}(X))^2}{\mathbf{E}(X^2)} .$$

Лемма 1. $\mathbf{E}(N(\tau)) \geqslant \beta' \sqrt{t} \frac{F}{E}$

Лемма 2. $\mathbf{E}(N(\tau)^2) \leqslant \beta'' \sqrt{t} \frac{F}{E}$ при $\frac{F}{E} < \frac{1}{\sqrt{t}}$

Из утверждения и лемм следует требуемое неравенство

$$\mathop{\mathbf{Pr}}_{\tau \leftarrow U}[N(\tau) > 0] > \beta \sqrt{t} \frac{F}{E} .$$

Оценка первого момента

Из линейности матожидания

$$\mathop{\mathbf{E}}_{\tau\leftarrow U}[N(\tau)] = \sum_{j=t-\delta\sqrt{t}}^{t+\delta\sqrt{t}} \mathop{\mathbf{Pr}}_{\tau\leftarrow U}[\tau_j \text{ ребро бракованное и существенное}].$$

При любом j для случайного маршрута j-е ребро распределено равномерно по E. (Граф G регулярный.)
Поэтому

$$\mathop{\mathbf{Pr}}_{\tau\leftarrow U}[\tau_j \text{ бракованное и существенное}] =$$

$$= \sum_{e\in F} \mathop{\mathbf{Pr}}_{\tau\leftarrow U}[\tau_j \text{ существенное} \mid \tau_j = e] \cdot \mathop{\mathbf{Pr}}_{\tau\leftarrow U}[\tau_j = e] \geqslant$$

$$\geqslant \frac{F}{E} \min_{e\in F} \mathop{\mathbf{Pr}}_{\tau\leftarrow U}[\tau_j \text{ существенное} \mid \tau_j = e]$$

Оценка первого момента

Из линейности матожидания

$$\mathop{\mathbf{E}}_{\tau\leftarrow U}[N(\tau)] = \sum_{j=t-\delta\sqrt{t}}^{t+\delta\sqrt{t}} \mathop{\mathbf{Pr}}_{\tau\leftarrow U}[\tau_j \text{ ребро бракованное и существенное}].$$

При любом j для случайного маршрута j-е ребро распределено равномерно по E. (Граф G регулярный.)

Поэтому

$$\mathop{\mathbf{Pr}}_{\tau\leftarrow U}[\tau_j \text{ бракованное и существенное}] =$$

$$= \sum_{e\in F} \mathop{\mathbf{Pr}}_{\tau\leftarrow U}[\tau_j \text{ существенное} \mid \tau_j = e] \cdot \mathop{\mathbf{Pr}}_{\tau\leftarrow U}[\tau_j = e] \geqslant$$

$$\geqslant \frac{F}{E} \min_{e\in F} \mathop{\mathbf{Pr}}_{\tau\leftarrow U}[\tau_j \text{ существенное} \mid \tau_j = e]$$

Оценка первого момента

Из линейности матожидания

$$\mathop{\mathbf{E}}_{\tau\leftarrow U}[N(\tau)] = \sum_{j=t-\delta\sqrt{t}}^{t+\delta\sqrt{t}} \mathop{\mathbf{Pr}}_{\tau\leftarrow U}[\tau_j \text{ ребро бракованное и существенное}].$$

При любом j для случайного маршрута j-е ребро распределено равномерно по E. (Граф G регулярный.)
Поэтому

$$\mathop{\mathbf{Pr}}_{\tau\leftarrow U}[\tau_j \text{ бракованное и существенное}] =$$

$$= \sum_{e\in F} \mathop{\mathbf{Pr}}_{\tau\leftarrow U}[\tau_j \text{ существенное} \mid \tau_j = e] \cdot \mathop{\mathbf{Pr}}_{\tau\leftarrow U}[\tau_j = e] \geqslant$$

$$\geqslant \frac{F}{E} \min_{e\in F} \mathop{\mathbf{Pr}}_{\tau\leftarrow U}[\tau_j \text{ существенное} \mid \tau_j = e]$$

Существенных ребер много в средней части

Утверждение

Существует такая константа C, что для любого $\delta < \frac{1}{C\Sigma}$ и для любого ребра e при $|j - t| \leqslant \delta\sqrt{t}$ выполняется

$$\Pr_{\tau \leftarrow U}[\tau_j \text{ существенное} \mid \tau_j = e] \geqslant \frac{1}{4\Sigma^2}\ .$$

Вывод леммы 1 из утверждения

$$\mathbf{E}_{\tau \leftarrow U}[N(\tau)] = \sum_{j=t-\delta\sqrt{t}}^{t+\delta\sqrt{t}} \Pr_{\tau \leftarrow U}[\tau_j \text{ бракованное и существенное}] \geqslant$$

$$\geqslant 2\delta\sqrt{t}\frac{F}{E}\frac{1}{4\Sigma^2} = \frac{\delta}{2\Sigma^2}\sqrt{t}\frac{F}{E}\ .$$

Существенных ребер много в средней части

Утверждение

Существует такая константа C, что для любого $\delta < \frac{1}{C\Sigma}$ и для любого ребра e при $|j - t| \leqslant \delta\sqrt{t}$ выполняется

$$\mathop{\mathbf{Pr}}_{\tau \leftarrow U}[\tau_j \text{ существенное} \mid \tau_j = e] \geqslant \frac{1}{4\Sigma^2} .$$

Вывод леммы 1 из утверждения

$$\mathop{\mathbf{E}}_{\tau \leftarrow U}[N(\tau)] = \sum_{j=t-\delta\sqrt{t}}^{t+\delta\sqrt{t}} \mathop{\mathbf{Pr}}_{\tau \leftarrow U}[\tau_j \text{ бракованное и существенное}] \geqslant$$

$$\geqslant 2\delta\sqrt{t}\frac{F}{E}\frac{1}{4\Sigma^2} = \frac{\delta}{2\Sigma^2}\sqrt{t}\frac{F}{E} .$$

Другой способ случайно выбрать маршрут

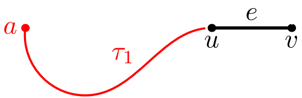
1. Выбираем случайно и равномерно ребро $e = (uv)$.
2. Выбираем случайно и равномерно $0 \leqslant j \leqslant 2t$.
3. Выбираем случайно и равномерно маршрут τ_1 длины j с началом u.
4. Выбираем случайно и равномерно маршрут τ_2 длины $2t - j$ с началом v.
5. Выдаем маршрут $\tau = (\tau_1)^R e \tau_2$.

Другой способ случайно выбрать маршрут

1. Выбираем случайно и равномерно ребро $e = (uv)$.
2. Выбираем случайно и равномерно $0 \leqslant j \leqslant 2t$.
3. Выбираем случайно и равномерно маршрут τ_1 длины j с началом u.
4. Выбираем случайно и равномерно маршрут τ_2 длины $2t - j$ с началом v.
5. Выдаем маршрут $\tau = (\tau_1)^R e \tau_2$.

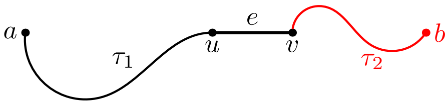
Другой способ случайно выбрать маршрут

1. Выбираем случайно и равномерно ребро $e = (uv)$.
2. Выбираем случайно и равномерно $0 \leqslant j \leqslant 2t$.
3. Выбираем случайно и равномерно маршрут τ_1 длины j с началом u.
4. Выбираем случайно и равномерно маршрут τ_2 длины $2t - j$ с началом v.
5. Выдаем маршрут $\tau = (\tau_1)^R e \tau_2$.



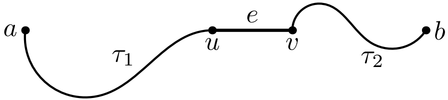
Другой способ случайно выбрать маршрут

1. Выбираем случайно и равномерно ребро $e = (uv)$.
2. Выбираем случайно и равномерно $0 \leqslant j \leqslant 2t$.
3. Выбираем случайно и равномерно маршрут τ_1 длины j с началом u.
4. Выбираем случайно и равномерно маршрут τ_2 длины $2t - j$ с началом v.
5. Выдаем маршрут $\tau = (\tau_1)^R e \tau_2$.



Другой способ случайно выбрать маршрут

1. Выбираем случайно и равномерно ребро $e = (uv)$.
2. Выбираем случайно и равномерно $0 \leqslant j \leqslant 2t$.
3. Выбираем случайно и равномерно маршрут τ_1 длины j с началом u.
4. Выбираем случайно и равномерно маршрут τ_2 длины $2t - j$ с началом v.
5. Выдаем маршрут $\tau = (\tau_1)^R e \tau_2$.



Среднее ребро

Пусть $j = t + 1$. Тогда конец a маршрута τ_1 распределен так же, как при голосовании. (Аналогично для конца b маршрута τ_2.)
Вероятность ответа большинства не меньше $1/\Sigma$ (общее число строк в бюллетене голосования).
Поэтому

$$\Pr_{\tau \leftarrow U}[\tau_{t+1} \text{ существенное} \mid \tau_{t+1} = e] =$$

$$\mathbf{Pr}[a \text{ голосует в } u \text{ за } \sigma(u)] \cdot \mathbf{Pr}[b \text{ голосует в } v \text{ за } \sigma(v)] \geqslant$$

$$\geqslant \frac{1}{\Sigma^2}.$$

Среднее ребро

Пусть $j = t + 1$. Тогда конец a маршрута τ_1 распределен так же, как при голосовании. (Аналогично для конца b маршрута τ_2.)
Вероятность ответа большинства не меньше $1/\Sigma$ (общее число строк в бюллетене голосования).
Поэтому

$$\Pr_{\tau \leftarrow U}[\tau_{t+1} \text{ существенное} \mid \tau_{t+1} = e] =$$
$$\Pr[a \text{ голосует в } u \text{ за } \sigma(u)] \cdot \Pr[b \text{ голосует в } v \text{ за } \sigma(v)] \geqslant$$
$$\geqslant \frac{1}{\Sigma^2}.$$

Среднее ребро

Пусть $j = t + 1$. Тогда конец a маршрута τ_1 распределен так же, как при голосовании. (Аналогично для конца b маршрута τ_2.)
Вероятность ответа большинства не меньше $1/\Sigma$ (общее число строк в бюллетене голосования).
Поэтому

$$\Pr_{\tau \leftarrow U}[\tau_{t+1} \text{ существенное} \mid \tau_{t+1} = e] =$$

$$\Pr[a \text{ голосует в } u \text{ за } \sigma(u)] \cdot \Pr[b \text{ голосует в } v \text{ за } \sigma(v)] \geqslant$$

$$\geqslant \frac{1}{\Sigma^2} .$$

Рёбра из средней части

Пусть $t - \delta\sqrt{t} < j < t + \delta\sqrt{t}$.
Распределение концов маршрутов τ_1 и τ_2 отличается от распределения при голосовании.
Но не очень сильно.
Половина ребер, инцидентных каждой вершине графа G, — петли.

Альтернативный способ построения маршрута

Чтобы построить случайный маршрут длины ℓ, начинающийся в вершине u:

1. построим случайное подмножество $S \subset [1..\ell]$, включая в него каждое число независимо с вероятностью $1/2$;
2. начиная с вершины u, сделаем $\ell - |S|$ шагов по ребрам графа G, каждый раз равновероятно выбирая одного из соседей, отличных от текущей вершины.

Рёбра из средней части

Пусть $t - \delta\sqrt{t} < j < t + \delta\sqrt{t}$.
Распределение концов маршрутов τ_1 и τ_2 отличается от распределения при голосовании.
Но не очень сильно.
Половина ребер, инцидентных каждой вершине графа G, — петли.

Альтернативный способ построения маршрута

Чтобы построить случайный маршрут длины ℓ, начинающийся в вершине u:

1. построим случайное подмножество $S \subset [1..\ell]$, включая в него каждое число независимо с вероятностью $1/2$;
2. начиная с вершины u, сделаем $\ell - |S|$ шагов по ребрам графа G, каждый раз равновероятно выбирая одного из соседей, отличных от текущей вершины.

Рёбра из средней части

Пусть $t - \delta\sqrt{t} < j < t + \delta\sqrt{t}$.
Распределение концов маршрутов τ_1 и τ_2 отличается от распределения при голосовании.
Но не очень сильно.
Половина ребер, инцидентных каждой вершине графа G, — петли.

Альтернативный способ построения маршрута

Чтобы построить случайный маршрут длины ℓ, начинающийся в вершине u:

1. построим случайное подмножество $S \subset [1..\ell]$, включая в него каждое число независимо с вероятностью $1/2$;
2. начиная с вершины u, сделаем $\ell - |S|$ шагов по ребрам графа G, каждый раз равновероятно выбирая одного из соседей, отличных от текущей вершины.

Рёбра из средней части

Пусть $t - \delta\sqrt{t} < j < t + \delta\sqrt{t}$.
Распределение концов маршрутов τ_1 и τ_2 отличается от распределения при голосовании.
Но не очень сильно.
Половина ребер, инцидентных каждой вершине графа G, — петли.

Альтернативный способ построения маршрута

Чтобы построить случайный маршрут длины ℓ, начинающийся в вершине u:

1. построим случайное подмножество $S \subset [1..\ell]$, включая в него каждое число независимо с вероятностью $1/2$;
2. начиная с вершины u, сделаем $\ell - |S|$ шагов по ребрам графа G, каждый раз равновероятно выбирая одного из соседей, отличных от текущей вершины.

Сравнение маршрутов близких длин

$p_\ell(u,a)$ — вероятность того, что случайный маршрут по графу G длины ℓ, начинающийся в u, заканчивается в a.
$q_\ell(u,a)$ — аналогичная вероятность для маршрутов, которые не проходят по петлям.
Альтернативный способ построения маршрута дает равенство

$$p_\ell(u,a) = \sum_{k=0}^{\ell} B(\ell,k) q_{\ell-k}(u,a).$$

Здесь $B(\ell,k)$ — биномиальное распределение $B(\ell,k) = \dfrac{\binom{\ell}{k}}{2^\ell}$.

Лемма о близости биномиальных распределений

Существует такая константа C, что для $t - \delta\sqrt{t} < j < t + \delta\sqrt{t}$ выполнено

$$\frac{1}{2}\sum_m |B(t,m) - B(j,m)| < \frac{C}{4}\delta.$$

Сравнение маршрутов близких длин

$p_\ell(u,a)$ — вероятность того, что случайный маршрут по графу G длины ℓ, начинающийся в u, заканчивается в a.
$q_\ell(u,a)$ — аналогичная вероятность для маршрутов, которые не проходят по петлям.
Альтернативный способ построения маршрута дает равенство

$$p_\ell(u,a) = \sum_{k=0}^{\ell} B(\ell,k) q_{\ell-k}(u,a).$$

Здесь $B(\ell,k)$ — биномиальное распределение $B(\ell,k) = \frac{\binom{\ell}{k}}{2^\ell}$.

Лемма о близости биномиальных распределений

Существует такая константа C, что для $t-\delta\sqrt{t} < j < t+\delta\sqrt{t}$ выполнено

$$\frac{1}{2}\sum_m |B(t,m) - B(j,m)| < \frac{C}{4}\delta.$$

Сравнение маршрутов близких длин

$p_\ell(u,a)$ — вероятность того, что случайный маршрут по графу G длины ℓ, начинающийся в u, заканчивается в a.
$q_\ell(u,a)$ — аналогичная вероятность для маршрутов, которые не проходят по петлям.
Альтернативный способ построения маршрута дает равенство

$$p_\ell(u,a) = \sum_{k=0}^{\ell} B(\ell,k) q_{\ell-k}(u,a).$$

Здесь $B(\ell,k)$ — биномиальное распределение $B(\ell,k) = \dfrac{\binom{\ell}{k}}{2^\ell}$.

Лемма о близости биномиальных распределений

Существует такая константа C, что для $t-\delta\sqrt{t} < j < t+\delta\sqrt{t}$ выполнено

$$\frac{1}{2}\sum_m |B(t,m) - B(j,m)| < \frac{C}{4}\delta.$$

Доказательство утверждения

Утверждение

Существует такая константа C, что для любого $\delta < \frac{1}{C\Sigma}$ и для любого ребра e при $|j - t| \leqslant \delta\sqrt{t}$ выполняется

$$\Pr_{\tau \leftarrow U}[\tau_j \text{ существенное} \mid \tau_j = e] \geqslant \frac{1}{4\Sigma^2} .$$

1. Из леммы о близости биномиальных распределений получаем
$$|p_j(u,a) - p_t(u,a)| < \frac{C}{2}\delta, \quad |p_{2t-j}(v,b) - p_t(v,b)| < \frac{C}{2}\delta.$$
2. Поэтому
$$\Pr_{\tau_1}[a \text{ голосует в } u \text{ за } \sigma(u)] > \frac{1}{\Sigma} - \frac{C}{2}\delta$$
(аналогично для вероятности того, что b голосует в v за $\sigma(v)$).
3. Значит, $\Pr_{\tau \leftarrow U}[\tau_j \text{ существенное} \mid \tau_j = e] > \left(\frac{1}{\Sigma} - \frac{C}{2}\delta\right)^2 > \frac{1}{4\Sigma^2}$.

Доказательство утверждения

Утверждение

Существует такая константа C, что для любого $\delta < \frac{1}{C\Sigma}$ и для любого ребра e при $|j - t| \leqslant \delta\sqrt{t}$ выполняется

$$\Pr_{\tau \leftarrow U}[\tau_j \text{ существенное} \mid \tau_j = e] \geqslant \frac{1}{4\Sigma^2} .$$

1. Из леммы о близости биномиальных распределений получаем

$$|p_j(u,a) - p_t(u,a)| < \frac{C}{2}\delta, \quad |p_{2t-j}(v,b) - p_t(v,b)| < \frac{C}{2}\delta.$$

2. Поэтому

$$\Pr_{\tau_1}[a \text{ голосует в } u \text{ за } \sigma(u)] > \frac{1}{\Sigma} - \frac{C}{2}\delta$$

(аналогично для вероятности того, что b голосует в v за $\sigma(v)$).

3. Значит, $\Pr_{\tau \leftarrow U}[\tau_j \text{ существенное} \mid \tau_j = e] > \left(\frac{1}{\Sigma} - \frac{C}{2}\delta\right)^2 > \frac{1}{4\Sigma^2}$.

Доказательство утверждения

Утверждение

Существует такая константа C, что для любого $\delta < \frac{1}{C\Sigma}$ и для любого ребра e при $|j - t| \leqslant \delta\sqrt{t}$ выполняется

$$\Pr_{\tau \leftarrow U}[\tau_j \text{ существенное} \mid \tau_j = e] \geqslant \frac{1}{4\Sigma^2}\ .$$

1. Из леммы о близости биномиальных распределений получаем
$$|p_j(u,a) - p_t(u,a)| < \frac{C}{2}\delta, \quad |p_{2t-j}(v,b) - p_t(v,b)| < \frac{C}{2}\delta.$$
2. Поэтому
$$\Pr_{\tau_1}[a \text{ голосует в } u \text{ за } \sigma(u)] > \frac{1}{\Sigma} - \frac{C}{2}\delta$$
(аналогично для вероятности того, что b голосует в v за $\sigma(v)$).
3. Значит, $\Pr_{\tau \leftarrow U}[\tau_j \text{ существенное} \mid \tau_j = e] > \left(\frac{1}{\Sigma} - \frac{C}{2}\delta\right)^2 > \frac{1}{4\Sigma^2}.$

Доказательство утверждения

Утверждение

Существует такая константа C, что для любого $\delta < \frac{1}{C\Sigma}$ и для любого ребра e при $|j - t| \leqslant \delta\sqrt{t}$ выполняется

$$\Pr_{\tau \leftarrow U}[\tau_j \text{ существенное} \mid \tau_j = e] \geqslant \frac{1}{4\Sigma^2}.$$

1. Из леммы о близости биномиальных распределений получаем
$$|p_j(u,a) - p_t(u,a)| < \frac{C}{2}\delta, \quad |p_{2t-j}(v,b) - p_t(v,b)| < \frac{C}{2}\delta.$$
2. Поэтому
$$\Pr_{\tau_1}[a \text{ голосует в } u \text{ за } \sigma(u)] > \frac{1}{\Sigma} - \frac{C}{2}\delta$$
(аналогично для вероятности того, что b голосует в v за $\sigma(v)$).
3. Значит, $\Pr_{\tau \leftarrow U}[\tau_j \text{ существенное} \mid \tau_j = e] > \left(\frac{1}{\Sigma} - \frac{C}{2}\delta\right)^2 > \frac{1}{4\Sigma^2}$.

Оценка второго момента

Лемма 2. $\mathbf{E}(N(\tau)^2) \leqslant \beta'' \sqrt{t}\frac{F}{E}$ при $\frac{F}{E} < \frac{1}{\sqrt{t}}$

$N(\tau)$ — количество бракованных существенных ребер в средней части маршрута τ.

$Z(\tau)$ — количество бракованных ребер там же.

$0 \leqslant N(\tau) \leqslant Z(\tau)$, значит $\mathbf{E}(N^2(\tau)) \leqslant \mathbf{E}(Z^2(\tau))$.

$Z_j(\tau)$ — характеристическая функция j-го бракованного ребра на маршруте τ.

Из линейности матожидания $(t - \delta\sqrt{t} < j < k < t + \delta\sqrt{t})$

$$\mathbf{E}(Z^2(\tau)) = \sum_j \mathbf{E}(Z_j^2(\tau)) + 2\sum_{j<k} \mathbf{E}(Z_j(\tau)Z_k(\tau)) =$$

$$= 2\delta\sqrt{t}\frac{F}{E} + 2\sum_{j<k} \mathbf{E}(Z_j(\tau)Z_k(\tau)).$$

Оценка второго момента

Лемма 2. $\mathbf{E}(N(\tau)^2) \leqslant \beta''\sqrt{t}\frac{F}{E}$ при $\frac{F}{E} < \frac{1}{\sqrt{t}}$

$N(\tau)$ — количество бракованных существенных ребер в средней части маршрута τ.

$Z(\tau)$ — количество бракованных ребер там же.

$0 \leqslant N(\tau) \leqslant Z(\tau)$, значит $\mathbf{E}(N^2(\tau)) \leqslant \mathbf{E}(Z^2(\tau))$.

$Z_j(\tau)$ — характеристическая функция j-го бракованного ребра на маршруте τ.

Из линейности матожидания $(t - \delta\sqrt{t} < j < k < t + \delta\sqrt{t})$

$$\mathbf{E}(Z^2(\tau)) = \sum_j \mathbf{E}(Z_j^2(\tau)) + 2\sum_{j<k} \mathbf{E}(Z_j(\tau)Z_k(\tau)) =$$

$$= 2\delta\sqrt{t}\frac{F}{E} + 2\sum_{j<k} \mathbf{E}(Z_j(\tau)Z_k(\tau)).$$

Оценка второго момента

Лемма 2. $\mathbf{E}(N(\tau)^2) \leqslant \beta''\sqrt{t}\frac{F}{E}$ при $\frac{F}{E} < \frac{1}{\sqrt{t}}$

$N(\tau)$ — количество бракованных существенных ребер в средней части маршрута τ.
$Z(\tau)$ — количество бракованных ребер там же.
$0 \leqslant N(\tau) \leqslant Z(\tau)$, значит $\mathbf{E}(N^2(\tau)) \leqslant \mathbf{E}(Z^2(\tau))$.
$Z_j(\tau)$ — характеристическая функция j-го бракованного ребра на маршруте τ.
Из линейности матожидания $(t - \delta\sqrt{t} < j < k < t + \delta\sqrt{t})$

$$\mathbf{E}(Z^2(\tau)) = \sum_j \mathbf{E}(Z_j^2(\tau)) + 2\sum_{j<k} \mathbf{E}(Z_j(\tau)Z_k(\tau)) =$$

$$= 2\delta\sqrt{t}\frac{F}{E} + 2\sum_{j<k} \mathbf{E}(Z_j(\tau)Z_k(\tau)).$$

Оценка второго момента (окончание)

$$\mathbf{E}(Z_j(\tau)Z_k(\tau)) = \mathbf{Pr}[\tau_k \in F \mid \tau_j \in F] \cdot \mathbf{Pr}[\tau_j \in F] = \frac{F}{E}\mathbf{Pr}[\tau_k \in F \mid \tau_j \in F]$$

Лемма 3. (Еще одно свойство экспандеров)

Если граф G — алгебраический (λ, d)-экспандер, то

$$\mathbf{Pr}[\tau_k \in F \mid \tau_j \in F] \leqslant \frac{F}{E} + \lambda^{k-j}.$$

Завершение доказательства леммы 2 $(t - \delta\sqrt{t} < j < k < t + \delta\sqrt{t})$:

$$\sum_{j<k} \mathbf{E}(Z_j(\tau)Z_k(\tau)) \leqslant \frac{F}{E}\sum_{j<k}\left(\frac{F}{E} + \lambda^{k-j}\right) \leqslant$$

$$\leqslant \frac{F}{E}\left(\frac{F}{E}(2\delta\sqrt{t})^2 + 2\delta\sqrt{t}\frac{\lambda}{1-\lambda}\right) = 2\delta\sqrt{t}\frac{F}{E}\left(\frac{F}{E}\cdot 2\delta\sqrt{t} + \frac{\lambda}{1-\lambda}\right) =$$

$$= \beta_1\sqrt{t}\frac{F}{E} \qquad \text{при } \frac{F}{E} < \frac{1}{\sqrt{t}}.$$

Оценка второго момента (окончание)

$$\mathbf{E}(Z_j(\tau)Z_k(\tau)) = \mathbf{Pr}[\tau_k \in F \mid \tau_j \in F] \cdot \mathbf{Pr}[\tau_j \in F] = \frac{F}{E}\mathbf{Pr}[\tau_k \in F \mid \tau_j \in F]$$

Лемма 3. (Еще одно свойство экспандеров)

Если граф G — алгебраический (λ, d)-экспандер, то

$$\mathbf{Pr}[\tau_k \in F \mid \tau_j \in F] \leqslant \frac{F}{E} + \lambda^{k-j}.$$

Завершение доказательства леммы 2 ($t - \delta\sqrt{t} < j < k < t + \delta\sqrt{t}$):

$$\sum_{j<k} \mathbf{E}(Z_j(\tau)Z_k(\tau)) \leqslant \frac{F}{E}\sum_{j<k}\left(\frac{F}{E} + \lambda^{k-j}\right) \leqslant$$

$$\leqslant \frac{F}{E}\left(\frac{F}{E}(2\delta\sqrt{t})^2 + 2\delta\sqrt{t}\frac{\lambda}{1-\lambda}\right) = 2\delta\sqrt{t}\frac{F}{E}\left(\frac{F}{E}\cdot 2\delta\sqrt{t} + \frac{\lambda}{1-\lambda}\right) =$$

$$= \beta_1\sqrt{t}\frac{F}{E} \qquad \text{при } \frac{F}{E} < \frac{1}{\sqrt{t}}.$$

Оценка второго момента (окончание)

$$\mathbf{E}(Z_j(\tau)Z_k(\tau)) = \mathbf{Pr}[\tau_k \in F \mid \tau_j \in F] \cdot \mathbf{Pr}[\tau_j \in F] = \frac{F}{E}\mathbf{Pr}[\tau_k \in F \mid \tau_j \in F]$$

Лемма 3. (Еще одно свойство экспандеров)

Если граф G — алгебраический (λ, d)-экспандер, то

$$\mathbf{Pr}[\tau_k \in F \mid \tau_j \in F] \leqslant \frac{F}{E} + \lambda^{k-j}.$$

Завершение доказательства леммы 2 ($t - \delta\sqrt{t} < j < k < t + \delta\sqrt{t}$):

$$\sum_{j<k} \mathbf{E}(Z_j(\tau)Z_k(\tau)) \leqslant \frac{F}{E}\sum_{j<k}\left(\frac{F}{E} + \lambda^{k-j}\right) \leqslant$$

$$\leqslant \frac{F}{E}\left(\frac{F}{E}(2\delta\sqrt{t})^2 + 2\delta\sqrt{t}\frac{\lambda}{1-\lambda}\right) = 2\delta\sqrt{t}\frac{F}{E}\left(\frac{F}{E}\cdot 2\delta\sqrt{t} + \frac{\lambda}{1-\lambda}\right) =$$

$$= \beta_1\sqrt{t}\frac{F}{E} \qquad \text{при } \frac{F}{E} < \frac{1}{\sqrt{t}}\ .$$

План

1 Увеличение зазора

2 Уменьшение алфавита: локально проверяемые коды

3 Преобразование k-выполнимости в 2-выполнимость

4 Улучшение графа

5 Выбор параметров

Длинный код

Определение

Длинный код — это отображение $L\colon \Sigma \to 2^{2^{\Sigma}}$, которое задается правилом

$$\sigma \mapsto A_\sigma, \qquad A_\sigma(f) = f(\sigma).$$

Длинный код сопоставляет символу из алфавита двоичный вектор (таблицу), позиции в котором индексированы отображениями $\Sigma \to \{0, 1\}$ (подмножествами Σ).

Мы будем также смотреть на эту таблицу как на отображение $\mathbb{F}_2^{\Sigma} \to \mathbb{F}_2$, где $\mathbb{F}_2$ — поле из двух элементов, $\mathbb{F}_2^{\Sigma}$ — прямая сумма (с покомпонентными операциями).

Лемма

Кодовые векторы длинного кода — это в точности гомоморфизмы колец $\mathbb{F}_2^{\Sigma} \to \mathbb{F}_2$.

Длинный код

Определение

Длинный код — это отображение $L\colon \Sigma \to 2^{2^{\Sigma}}$, которое задается правилом

$$\sigma \mapsto A_\sigma, \qquad A_\sigma(f) = f(\sigma).$$

Длинный код сопоставляет символу из алфавита двоичный вектор (таблицу), позиции в котором индексированы отображениями $\Sigma \to \{0,1\}$ (подмножествами Σ).

Мы будем также смотреть на эту таблицу как на отображение $\mathbb{F}_2^{\Sigma} \to \mathbb{F}_2$, где $\mathbb{F}_2$ — поле из двух элементов, $\mathbb{F}_2^{\Sigma}$ — прямая сумма (с покомпонентными операциями).

Лемма

Кодовые векторы длинного кода — это в точности гомоморфизмы колец $\mathbb{F}_2^{\Sigma} \to \mathbb{F}_2$.

Длинный код

Определение

Длинный код — это отображение $L\colon \Sigma \to 2^{2^\Sigma}$, которое задается правилом

$$\sigma \mapsto A_\sigma, \qquad A_\sigma(f) = f(\sigma).$$

Длинный код сопоставляет символу из алфавита двоичный вектор (таблицу), позиции в котором индексированы отображениями $\Sigma \to \{0,1\}$ (подмножествами Σ).

Мы будем также смотреть на эту таблицу как на отображение $\mathbb{F}_2^\Sigma \to \mathbb{F}_2$, где $\mathbb{F}_2$ — поле из двух элементов, $\mathbb{F}_2^\Sigma$ — прямая сумма (с покомпонентными операциями).

Лемма

Кодовые векторы длинного кода — это в точности гомоморфизмы колец $\mathbb{F}_2^\Sigma \to \mathbb{F}_2$.

Уменьшение алфавита: проверки в длинном коде

- Исходный граф $G(V, E, \Sigma, c)$. По нему строим гиперграф $H(V', E', \{0,1\}, c')$ арности 10 ($k = 10$).
- Ограничения $c(u, v)$ рассматриваем как функции $\Sigma^2 \to \mathbb{F}_2$.
- Новые переменные ($2^{\Sigma} V + 2^{\Sigma^2} E$ штук):
  - таблицы $B_v(r)$, $v \in V$, $r\colon \Sigma \to \mathbb{F}_2$;
  - таблицы $A_{u,v}(f)$, $(u,v) \in E$, $f\colon \Sigma^2 \to \mathbb{F}_2$;
- Новые ограничения индексированы f, g, h, r и $(u, v) \in E$ ($2^{3\Sigma^2 + \Sigma} E$ штук):

$$
\bigwedge \begin{cases}
A_{u,v}(f+g) = A_{u,v}(f) + A_{u,v}(g), & \\
A_{u,v}(fg+h) = A_{u,v}(f)A_{u,v}(g) + A_{u,v}(h), & \\
A_{u,v}(r_1+h) = B_u(r) + A_{u,v}(h), & r_1(x,y) = r(x) \\
A_{u,v}(h+r_2) = A_{u,v}(h) + B_v(r), & r_2(x,y) = r(y) \\
A_{u,v}(c(u,v)+h) = 1 + A_{u,v}(h). &
\end{cases}
$$

Уменьшение алфавита: проверки в длинном коде

- Исходный граф $G(V, E, \Sigma, c)$. По нему строим гиперграф $H(V', E', \{0,1\}, c')$ арности 10 ($k = 10$).
- Ограничения $c(u, v)$ рассматриваем как функции $\Sigma^2 \to \mathbb{F}_2$.
- Новые переменные ($2^\Sigma V + 2^{\Sigma^2} E$ штук):
  - таблицы $B_v(r)$, $v \in V$, $r : \Sigma \to \mathbb{F}_2$;
  - таблицы $A_{u,v}(f)$, $(u,v) \in E$, $f : \Sigma^2 \to \mathbb{F}_2$.
- Новые ограничения индексированы f, g, h, r и $(u, v) \in E$ ($2^{3\Sigma^2+\Sigma} E$ штук):

$$
\bigwedge \begin{cases}
A_{u,v}(f+g) = A_{u,v}(f) + A_{u,v}(g), & \\
A_{u,v}(fg+h) = A_{u,v}(f)A_{u,v}(g) + A_{u,v}(h), & \\
A_{u,v}(r_1+h) = B_u(r) + A_{u,v}(h), & r_1(x,y) = r(x) \\
A_{u,v}(h+r_2) = A_{u,v}(h) + B_v(r), & r_2(x,y) = r(y) \\
A_{u,v}(c(u,v)+h) = 1 + A_{u,v}(h). &
\end{cases}
$$

Уменьшение алфавита: проверки в длинном коде

- Исходный граф $G(V, E, \Sigma, c)$. По нему строим гиперграф $H(V', E', \{0,1\}, c')$ арности 10 ($k = 10$).
- Ограничения $c(u, v)$ рассматриваем как функции $\Sigma^2 \to \mathbb{F}_2$.
- Новые переменные ($2^\Sigma V + 2^{\Sigma^2} E$ штук):
  - таблицы $B_v(r)$, $v \in V$, $r : \Sigma \to \mathbb{F}_2$;
  - таблицы $A_{u,v}(f)$, $(u, v) \in E$, $f : \Sigma^2 \to \mathbb{F}_2$;
- Новые ограничения индексированы f, g, h, r и $(u, v) \in E$ ($2^{3\Sigma^2 + \Sigma} E$ штук):

$$\bigwedge \begin{cases} A_{u,v}(f+g) = A_{u,v}(f) + A_{u,v}(g), & \\ A_{u,v}(fg+h) = A_{u,v}(f)A_{u,v}(g) + A_{u,v}(h), & \\ A_{u,v}(r_1+h) = B_u(r) + A_{u,v}(h), & r_1(x,y) = r(x) \\ A_{u,v}(h+r_2) = A_{u,v}(h) + B_v(r), & r_2(x,y) = r(y) \\ A_{u,v}(c(u,v)+h) = 1 + A_{u,v}(h). & \end{cases}$$

Уменьшение алфавита: проверки в длинном коде

- Исходный граф $G(V, E, \Sigma, c)$. По нему строим гиперграф $H(V', E', \{0, 1\}, c')$ арности 10 ($k = 10$).
- Ограничения $c(u, v)$ рассматриваем как функции $\Sigma^2 \to \mathbb{F}_2$.
- Новые переменные ($2^{\Sigma} V + 2^{\Sigma^2} E$ штук):
  - таблицы $B_v(r)$, $v \in V$, $r \colon \Sigma \to \mathbb{F}_2$;
  - таблицы $A_{u,v}(f)$, $(u, v) \in E$, $f \colon \Sigma^2 \to \mathbb{F}_2$;
- Новые ограничения индексированы f, g, h, r и $(u, v) \in E$ ($2^{3\Sigma^2+\Sigma} E$ штук):

$$\bigwedge \begin{cases} A_{u,v}(f+g) = A_{u,v}(f) + A_{u,v}(g), & \\ A_{u,v}(fg+h) = A_{u,v}(f)A_{u,v}(g) + A_{u,v}(h), & \\ A_{u,v}(r_1+h) = B_u(r) + A_{u,v}(h), & r_1(x,y) = r(x) \\ A_{u,v}(h+r_2) = A_{u,v}(h) + B_v(r), & r_2(x,y) = r(y) \\ A_{u,v}(c(u,v)+h) = 1 + A_{u,v}(h). & \end{cases}$$

Уменьшение алфавита: проверки в длинном коде

- Исходный граф $G(V, E, \Sigma, c)$. По нему строим гиперграф $H(V', E', \{0,1\}, c')$ арности 10 ($k = 10$).
- Ограничения $c(u, v)$ рассматриваем как функции $\Sigma^2 \to \mathbb{F}_2$.
- Новые переменные ($2^{\Sigma} V + 2^{\Sigma^2} E$ штук):
  - таблицы $B_v(r)$, $v \in V$, $r\colon \Sigma \to \mathbb{F}_2$;
  - таблицы $A_{u,v}(f)$, $(u, v) \in E$, $f\colon \Sigma^2 \to \mathbb{F}_2$;
- Новые ограничения индексированы f, g, h, r и $(u, v) \in E$ ($2^{3\Sigma^2+\Sigma}E$ штук):

$$\bigwedge \begin{cases} A_{u,v}(f+g) = A_{u,v}(f) + A_{u,v}(g), & \\ A_{u,v}(fg+h) = A_{u,v}(f)A_{u,v}(g) + A_{u,v}(h), & \\ A_{u,v}(r_1+h) = B_u(r) + A_{u,v}(h), & r_1(x,y) = r(x) \\ A_{u,v}(h+r_2) = A_{u,v}(h) + B_v(r), & r_2(x,y) = r(y) \\ A_{u,v}(c(u,v)+h) = 1 + A_{u,v}(h). & \end{cases}$$

Уменьшение алфавита: проверки в длинном коде

- Исходный граф $G(V, E, \Sigma, c)$. По нему строим гиперграф $H(V', E', \{0,1\}, c')$ арности 10 ($k = 10$).
- Ограничения $c(u, v)$ рассматриваем как функции $\Sigma^2 \to \mathbb{F}_2$.
- Новые переменные ($2^{\Sigma} V + 2^{\Sigma^2} E$ штук):
  - таблицы $B_v(r)$, $v \in V$, $r \colon \Sigma \to \mathbb{F}_2$;
  - таблицы $A_{u,v}(f)$, $(u, v) \in E$, $f \colon \Sigma^2 \to \mathbb{F}_2$;
- Новые ограничения индексированы f, g, h, r и $(u, v) \in E$ ($2^{3\Sigma^2+\Sigma} E$ штук):

$$\bigwedge \begin{cases} A_{u,v}(f+g) = A_{u,v}(f) + A_{u,v}(g), & \\ A_{u,v}(fg+h) = A_{u,v}(f)A_{u,v}(g) + A_{u,v}(h), & \\ A_{u,v}(r_1+h) = B_u(r) + A_{u,v}(h), & r_1(x,y) = r(x) \\ A_{u,v}(h+r_2) = A_{u,v}(h) + B_v(r), & r_2(x,y) = r(y) \\ A_{u,v}(c(u,v)+h) = 1 + A_{u,v}(h). & \end{cases}$$

Уменьшение алфавита: проверки в длинном коде

- Исходный граф $G(V, E, \Sigma, c)$. По нему строим гиперграф $H(V', E', \{0, 1\}, c')$ арности 10 ($k = 10$).
- Ограничения $c(u, v)$ рассматриваем как функции $\Sigma^2 \to \mathbb{F}_2$.
- Новые переменные ($2^{\Sigma} V + 2^{\Sigma^2} E$ штук):
  - таблицы $B_v(r)$, $v \in V$, $r \colon \Sigma \to \mathbb{F}_2$;
  - таблицы $A_{u,v}(f)$, $(u, v) \in E$, $f \colon \Sigma^2 \to \mathbb{F}_2$;
- Новые ограничения индексированы f, g, h, r и $(u, v) \in E$ ($2^{3\Sigma^2+\Sigma} E$ штук):

$$\bigwedge \begin{cases} A_{u,v}(f+g) = A_{u,v}(f) + A_{u,v}(g), & \\ A_{u,v}(fg+h) = A_{u,v}(f)A_{u,v}(g) + A_{u,v}(h), & \\ A_{u,v}(r_1+h) = B_u(r) + A_{u,v}(h), & r_1(x,y) = r(x) \\ A_{u,v}(h+r_2) = A_{u,v}(h) + B_v(r), & r_2(x,y) = r(y) \\ A_{u,v}(c(u,v)+h) = 1 + A_{u,v}(h). & \end{cases}$$

Оценка зазора

Теорема

Для некоторой константы β_3 выполняются неравенства

$$\beta_3 \mathrm{UNSAT}(G) \leqslant \mathrm{UNSAT}(H) \leqslant \mathrm{UNSAT}(G).$$

Оценка зазора: простая часть

$$\bigwedge \begin{cases} A_{u,v}(f+g) = A_{u,v}(f) + A_{u,v}(g), & \\ A_{u,v}(fg+h) = A_{u,v}(f)A_{u,v}(g) + A_{u,v}(h), & \\ A_{u,v}(r_1+h) = B_u(r) + A_{u,v}(h), & r_1(x,y) = r(x) \\ A_{u,v}(h+r_2) = A_{u,v}(h) + B_v(r), & r_2(x,y) = r(y) \\ A_{u,v}(c(u,v)+h) = 1 + A_{u,v}(h). & \end{cases}$$

Доказательство второго неравенства

По присваиванию σ в G построим в H присваивание σ':

$$A_{u,v} = L(\sigma(u), \sigma(v)), \quad B_u = L(\sigma(u)).$$

При таком присваивании первые четыре члена конъюнкции выполнены для любого ограничения $(f, g, h, r, (u,v))$. А последние члены выполнены, если выполнено $c(u,v)$. Поэтому $\text{UNSAT}_{\sigma'}(H) = \text{UNSAT}_{\sigma}(G)$. Значит, $\text{UNSAT}(H) \leqslant \text{UNSAT}(G)$.

Оценка зазора: простая часть

$$\bigwedge \begin{cases} A_{u,v}(f+g) = A_{u,v}(f) + A_{u,v}(g), & \\ A_{u,v}(fg+h) = A_{u,v}(f)A_{u,v}(g) + A_{u,v}(h), & \\ A_{u,v}(r_1+h) = B_u(r) + A_{u,v}(h), & r_1(x,y) = r(x) \\ A_{u,v}(h+r_2) = A_{u,v}(h) + B_v(r), & r_2(x,y) = r(y) \\ A_{u,v}(c(u,v)+h) = 1 + A_{u,v}(h). & \end{cases}$$

Доказательство второго неравенства

По присваиванию σ в G построим в H присваивание σ':

$$A_{u,v} = L(\sigma(u), \sigma(v)), \quad B_u = L(\sigma(u)).$$

При таком присваивании первые четыре члена конъюнкции выполнены для любого ограничения $(f, g, h, r, (u,v))$. А последние члены выполнены, если выполнено $c(u,v)$. Поэтому $\mathrm{UNSAT}_{\sigma'}(H) = \mathrm{UNSAT}_{\sigma}(G)$. Значит, $\mathrm{UNSAT}(H) \leqslant \mathrm{UNSAT}(G)$.

Оценка зазора: трудная часть

Основная лемма

Пусть $\sigma' = (A_{u,v}, B_u)$ нарушает долю δ ограничений H. Тогда найдется присваивание σ, которое нарушает не более 22δ ограничений G.

План доказательства

1. Если σ' нарушает мало ограничений H, то присваивание близко к длинному коду $L(\sigma)$.
2. Этот код $L(\sigma)$ также нарушает небольшую долю ограничений H.
3. Поэтому и соответствующее ему присваивание σ нарушает небольшую долю ограничений G.

Оценка зазора: трудная часть

Основная лемма

Пусть $\sigma' = (A_{u,v}, B_u)$ нарушает долю δ ограничений H. Тогда найдется присваивание σ, которое нарушает не более 22δ ограничений G.

План доказательства

1. Если σ' нарушает мало ограничений H, то присваивание близко к длинному коду $L(\sigma)$.
2. Этот код $L(\sigma)$ также нарушает небольшую долю ограничений H.
3. Поэтому и соответствующее ему присваивание σ нарушает небольшую долю ограничений G.

Длинный код, близкий к присваиванию

Пусть $\sigma' = (A_{u,v}, B_u)$ нарушает долю δ ограничений H.

Коррекция значений по большинству

$$\begin{cases} \tilde{A}_{u,v}(f) = \text{ самое частое значение } A_{u,v}(f+h) - A_{u,v}(h), \\ \tilde{B}_u(r) = \tilde{A}_{u,v}(r_1), \quad r_1(x,y) = r(x). \end{cases}$$

На ребре (u, v) нарушается минимум (по v) ограничений.

Наблюдение

Доля ребер $(u, v) \in E(G)$, для которых нарушается более ε доли (u, v)-ограничений H, не больше δ/ε.

Определение

Ребро $(u, v) \in E(G)$ назовем хорошим, если присваивание σ' нарушает не более $1/22$ (u, v)-ограничений H.

Длинный код, близкий к присваиванию

Пусть $\sigma' = (A_{u,v}, B_u)$ нарушает долю δ ограничений H.

Коррекция значений по большинству

$$\begin{cases} \tilde{A}_{u,v}(f) = \text{ самое частое значение } A_{u,v}(f+h) - A_{u,v}(h), \\ \tilde{B}_u(r) = \tilde{A}_{u,v}(r_1), \quad r_1(x,y) = r(x). \end{cases}$$

На ребре (u, v) нарушается минимум (по v) ограничений.

Наблюдение

Доля ребер $(u, v) \in E(G)$, для которых нарушается более ε доли (u, v)-ограничений H, не больше δ/ε.

Определение

Ребро $(u, v) \in E(G)$ назовем *хорошим*, если присваивание σ' нарушает не более $1/22$ (u, v)-ограничений H.

Длинный код, близкий к присваиванию

Пусть $\sigma' = (A_{u,v}, B_u)$ нарушает долю δ ограничений H.

Коррекция значений по большинству

$$\begin{cases} \tilde{A}_{u,v}(f) = \text{ самое частое значение } A_{u,v}(f+h) - A_{u,v}(h), \\ \tilde{B}_u(r) = \tilde{A}_{u,v}(r_1), \quad r_1(x,y) = r(x). \end{cases}$$

На ребре (u, v) нарушается минимум (по v) ограничений.

Наблюдение

Доля ребер $(u, v) \in E(G)$, для которых нарушается более ε доли (u, v)-ограничений H, не больше δ/ε.

Определение

Ребро $(u, v) \in E(G)$ назовем хорошим, если присваивание σ' нарушает не более $1/22$ (u, v)-ограничений H.

Свойства скорректированного присваивания

Лемма о квалифицированном большинстве

Для хорошего ребра $\Pr_h[\tilde{A}(f) = A(f+h) - A(h)] > \dfrac{10}{11}$.

$$\Pr_h[\tilde{A}(f) = A(f+h) - A(h)] = b_{f,\max} \geqslant b_{f,0}^2 + b_{f,1}^2 =$$

$$= \Pr_{g,h}[A(f+g) - A(g) = A(f+h) - A(h)] =$$

$$= \Pr_{g,h}[A(f+g) - A(f+h) = A(g) - A(h)] \geqslant$$

$$\geqslant \Pr_{g,h}[(A(f+g) - A(f+h) = A(g-h)) \wedge (A(g) - A(h) = A(g-h))] \geqslant \frac{10}{11} .$$

Свойства скорректированного присваивания

Лемма о квалифицированном большинстве

Для хорошего ребра $\Pr_h[\tilde{A}(f) = A(f+h) - A(h)] > \dfrac{10}{11}$.

$b_{f,a} = \mathbf{Pr}_h[a = A(f+h) - A(h)].$

$$\Pr_h[\tilde{A}(f) = A(f+h) - A(h)] = b_{f,\max} \geqslant b_{f,0}^2 + b_{f,1}^2 =$$

$$= \Pr_{g,h}[A(f+g) - A(g) = A(f+h) - A(h)] =$$

$$= \Pr_{g,h}[A(f+g) - A(f+h) = A(g) - A(h)] \geqslant$$

$$\geqslant \Pr_{g,h}[(A(f+g) - A(f+h) = A(g-h)) \wedge (A(g) - A(h) = A(g-h))] \geqslant \frac{10}{11}.$$

Свойства скорректированного присваивания

Лемма о квалифицированном большинстве

Для хорошего ребра $\Pr_h[\tilde{A}(f) = A(f+h) - A(h)] > \dfrac{10}{11}$.

$b_{f,a} = \mathbf{Pr}_h[a = A(f+h) - A(h)]$.
$b_{f,0} + b_{f,1} = 1$.

$$\Pr_h[\tilde{A}(f) = A(f+h) - A(h)] = b_{f,\max} \geqslant b_{f,0}^2 + b_{f,1}^2 =$$

$$= \Pr_{g,h}[A(f+g) - A(g) = A(f+h) - A(h)] =$$

$$= \Pr_{g,h}[A(f+g) - A(f+h) = A(g) - A(h)] \geqslant$$

$$\geqslant \Pr_{g,h}[(A(f+g) - A(f+h) = A(g-h)) \wedge (A(g) - A(h) = A(g-h))] \geqslant \frac{10}{11}.$$

Свойства скорректированного присваивания

Лемма о квалифицированном большинстве

Для хорошего ребра $\Pr_h[\tilde{A}(f) = A(f+h) - A(h)] > \dfrac{10}{11}$.

$\mathbf{Pr}[A = B] = \mathbf{Pr}[A = 0]\,\mathbf{Pr}[B = 0] + \mathbf{Pr}[A = 1]\,\mathbf{Pr}[B = 1]$ для независимых A, B.

$$\Pr_h[\tilde{A}(f) = A(f+h) - A(h)] = b_{f,\max} \geqslant b_{f,0}^2 + b_{f,1}^2 =$$

$$= \Pr_{g,h}[A(f+g) - A(g) = A(f+h) - A(h)] =$$

$$= \Pr_{g,h}[A(f+g) - A(f+h) = A(g) - A(h)] \geqslant$$

$$\geqslant \Pr_{g,h}[(A(f+g) - A(f+h) = A(g-h)) \wedge (A(g) - A(h) = A(g-h))] \geqslant \frac{10}{11}.$$

Свойства скорректированного присваивания

Лемма о квалифицированном большинстве

Для хорошего ребра $\Pr_h[\tilde{A}(f) = A(f+h) - A(h)] > \frac{10}{11}$.

Очевидно.

$$\Pr_h[\tilde{A}(f) = A(f+h) - A(h)] = b_{f,\max} \geqslant b_{f,0}^2 + b_{f,1}^2 =$$
$$= \Pr_{g,h}[A(f+g) - A(g) = A(f+h) - A(h)] =$$
$$= \Pr_{g,h}[A(f+g) - A(f+h) = A(g) - A(h)] \geqslant$$
$$\geqslant \Pr_{g,h}[(A(f+g) - A(f+h) = A(g-h)) \wedge (A(g) - A(h) = A(g-h))] \geqslant \frac{10}{11}.$$

Свойства скорректированного присваивания

Лемма о квалифицированном большинстве

Для хорошего ребра $\Pr_h[\tilde{A}(f) = A(f+h) - A(h)] > \dfrac{10}{11}$.

Каждое из условий выполняется столь же часто, как и условие линейности $A(f) + A(g) = A(f+g)$ (замена переменных), которое для хорошего ребра выполняется с вероятностью не меньше $21/22$.

$$\Pr_h[\tilde{A}(f) = A(f+h) - A(h)] = b_{f,\max} \geqslant b_{f,0}^2 + b_{f,1}^2 =$$

$$= \Pr_{g,h}[A(f+g) - A(g) = A(f+h) - A(h)] =$$

$$= \Pr_{g,h}[A(f+g) - A(f+h) = A(g) - A(h)] \geqslant$$

$$\geqslant \Pr_{g,h}[(A(f+g) - A(f+h) = A(g-h)) \wedge (A(g) - A(h) = A(g-h))] \geqslant \frac{10}{11}.$$

Свойства скорректированного присваивания (2)

Лемма о линейности

Для хорошего ребра $\tilde{A}(f)$ — линейная функция.

Из леммы о квалифицированном большинстве получаем заменами переменных

$$\Pr_h[\tilde{A}(f) = A(f+h) - A(h)] > \frac{10}{11},$$

$$\Pr_h[\tilde{A}(g) = A(f+g+h) - A(f+h)] > \frac{10}{11},$$

$$\Pr_h[\tilde{A}(f+g) = A(f+g+h) - A(h)] > \frac{10}{11}.$$

Одновременно все три события происходят с вероятностью не менее 8/11. Значит, для некоторого h' имеем

$$\tilde{A}(f) + \tilde{A}(g) = A(f+g+h') - A(h') = \tilde{A}(f+g).$$

Свойства скорректированного присваивания (2)

Лемма о линейности

Для хорошего ребра $\tilde{A}(f)$ — линейная функция.

Из леммы о квалифицированном большинстве получаем заменами переменных

$$\Pr_h[\tilde{A}(f) = A(f+h) - A(h)] > \frac{10}{11},$$
$$\Pr_h[\tilde{A}(g) = A(f+g+h) - A(f+h)] > \frac{10}{11},$$
$$\Pr_h[\tilde{A}(f+g) = A(f+g+h) - A(h)] > \frac{10}{11}.$$

Одновременно все три события происходят с вероятностью не менее $8/11$. Значит, для некоторого h' имеем

$$\tilde{A}(f) + \tilde{A}(g) = A(f+g+h') - A(h') = \tilde{A}(f+g).$$

Свойства скорректированного присваивания (2)

Лемма о линейности

Для хорошего ребра $\tilde{A}(f)$ — линейная функция.

Из леммы о квалифицированном большинстве получаем заменами переменных

$$\Pr_h[\tilde{A}(f) = A(f+h) - A(h)] > \frac{10}{11},$$

$$\Pr_h[\tilde{A}(g) = A(f+g+h) - A(f+h)] > \frac{10}{11},$$

$$\Pr_h[\tilde{A}(f+g) = A(f+g+h) - A(h)] > \frac{10}{11}.$$

Одновременно все три события происходят с вероятностью не менее $8/11$. Значит, для некоторого h' имеем

$$\tilde{A}(f) + \tilde{A}(g) = A(f+g+h') - A(h') = \tilde{A}(f+g).$$

Свойства скорректированного присваивания (3)

Лемма о близости

Для хорошего ребра $\Pr_f[\tilde{A}(f) \neq A(f)] < \dfrac{1}{20}$.

На хорошем ребре условие линейности нарушается редко. Применяя лемму о квалифицированном большинстве, получаем

$$\frac{1}{22} > \Pr_{f,g}[A(f+g) - A(g) \neq A(f)] \geqslant$$
$$\geqslant \Pr_{f,g}[(\tilde{A}(f) = A(f+g) - A(g)) \wedge (\tilde{A}(f) \neq A(f))] >$$
$$> \frac{20}{22} \Pr_f[\tilde{A}(f) \neq A(f)].$$

Свойства скорректированного присваивания (3)

Лемма о близости

Для хорошего ребра $\Pr_f[\tilde{A}(f) \neq A(f)] < \dfrac{1}{20}$.

На хорошем ребре условие линейности нарушается редко. Применяя лемму о квалифицированном большинстве, получаем

$$\frac{1}{22} > \Pr_{f,g}[A(f+g) - A(g) \neq A(f)] \geqslant$$
$$\geqslant \Pr_{f,g}[(\tilde{A}(f) = A(f+g) - A(g)) \wedge (\tilde{A}(f) \neq A(f))] >$$
$$> \frac{20}{22} \Pr_f[\tilde{A}(f) \neq A(f)].$$

Свойства скорректированного присваивания (4)

Лемма о кольцевом гомоморфизме

Для хорошего ребра $\tilde{A}(f)$ — гомоморфизм кольца $\mathbb{F}_2^{\Sigma^2}$ в поле $\mathbb{F}_2$:

$$\tilde{A}(fg) = \tilde{A}(f)\tilde{A}(g).$$

Следствие

Для хорошего ребра $\tilde{A}(f) = L((\sigma_1, \sigma_2))$ (код пары символов Σ).

Утверждение (отделенность гомоморфизмов)

Если линейное отображение $F\colon \mathbb{F}_2^N \to \mathbb{F}_2$ не является гомоморфизмом, то

$$\frac{5}{8} \geq \Pr_{f,g}[F(fg) \neq F(f)F(g)] \geq \frac{3}{8} > \frac{1}{4}.$$

Свойства скорректированного присваивания (4)

Лемма о кольцевом гомоморфизме

Для хорошего ребра $\tilde{A}(f)$ — гомоморфизм кольца $\mathbb{F}_2^{\Sigma^2}$ в поле $\mathbb{F}_2$:

$$\tilde{A}(fg) = \tilde{A}(f)\tilde{A}(g).$$

Следствие

Для хорошего ребра $\tilde{A}(f) = L((\sigma_1, \sigma_2))$ (код пары символов Σ).

Утверждение (отделенность гомоморфизмов)

Если линейное отображение $F\colon \mathbb{F}_2^N \to \mathbb{F}_2$ не является гомоморфизмом, то

$$\frac{5}{8} \geq \Pr_{f,g}[F(fg) \neq F(f)F(g)] \geq \frac{3}{8} > \frac{1}{4}.$$

Свойства скорректированного присваивания (4)

Лемма о кольцевом гомоморфизме

Для хорошего ребра $\tilde{A}(f)$ — гомоморфизм кольца $\mathbb{F}_2^{\Sigma^2}$ в поле $\mathbb{F}_2$:

$$\tilde{A}(fg) = \tilde{A}(f)\tilde{A}(g).$$

Следствие

Для хорошего ребра $\tilde{A}(f) = L((\sigma_1, \sigma_2))$ (код пары символов Σ).

Утверждение (отделенность гомоморфизмов)

Если линейное отображение $F\colon \mathbb{F}_2^N \to \mathbb{F}_2$ не является гомоморфизмом, то

$$\frac{5}{8} \geqslant \Pr_{f,g}[F(fg) \neq F(f)F(g)] \geqslant \frac{3}{8} > \frac{1}{4}.$$

Доказательство леммы о кольцевом гомоморфизме

Аналогично предыдущему применяем лемму о близости:

$$\Pr_{f,g,h}[\tilde{A}(fg+h) \neq \tilde{A}(f)\tilde{A}(g)+\tilde{A}(h)] \leqslant$$

$$\leqslant \Pr_{f,g,h}[A(fg+h) \neq A(f)A(g)+A(h)] + \Pr_{f,g,h}[\tilde{A}(fg+h) \neq A(fg+h)] +$$

$$+ \Pr_{f}[\tilde{A}(f) \neq A(f)] + \Pr_{g}[\tilde{A}(g) \neq A(g)] + \Pr_{h}[\tilde{A}(h) \neq A(h)] <$$

$$< \frac{1}{22} + \frac{4}{20} < \frac{1}{4}\,.$$

Теперь из отделенности гомоморфизмов следует, что $\tilde{A}$ — гомоморфизм.

Доказательство леммы о кольцевом гомоморфизме

Аналогично предыдущему применяем лемму о близости:

$$\Pr_{f,g,h}[\tilde{A}(fg+h) \neq \tilde{A}(f)\tilde{A}(g) + \tilde{A}(h)] \leqslant$$

$$\leqslant \Pr_{f,g,h}[A(fg+h) \neq A(f)A(g) + A(h)] + \Pr_{f,g,h}[\tilde{A}(fg+h) \neq A(fg+h)] +$$

$$+ \Pr_{f}[\tilde{A}(f) \neq A(f)] + \Pr_{g}[\tilde{A}(g) \neq A(g)] + \Pr_{h}[\tilde{A}(h) \neq A(h)] <$$

$$< \frac{1}{22} + \frac{4}{20} < \frac{1}{4}.$$

Теперь из отделенности гомоморфизмов следует, что $\tilde{A}$ — гомоморфизм.

Согласование в вершинах

По определению, $\tilde{B}_u(r) = \tilde{A}_{u,v}(r_1)$.

Если $\tilde{A}_{u,v}$ является кодом пары (σ_1, σ_2), то $\tilde{B}_u$ является кодом σ_1.

Отсюда получаем: если $\tilde{A}_{u,v}$ кодирует (σ_1, σ_2), а $\tilde{A}_{u,w}$ кодирует (σ_3, σ_4), причем $\sigma_1 \neq \sigma_3$, то

$$\Pr_{r,h}[\tilde{A}_{u,w}(r_1 + h) \neq \tilde{B}_u(r) + \tilde{A}_{u,w}(h)] \geqslant \frac{1}{2} \qquad (*)$$

(выполняется при $r(\sigma_1) \neq r(\sigma_3)$).

Лемма о согласовании

Для любого хорошего ребра (u, w), где $\tilde{B}_u$ кодирует σ_1, а $\tilde{B}_w$ кодирует σ_2, $\tilde{A}_{u,w}$ кодирует пару (σ_1, σ_2).

Согласование в вершинах

По определению, $\tilde{B}_u(r) = \tilde{A}_{u,v}(r_1)$.
Если $\tilde{A}_{u,v}$ является кодом пары (σ_1, σ_2), то $\tilde{B}_u$ является кодом σ_1.
Отсюда получаем: если $\tilde{A}_{u,v}$ кодирует (σ_1, σ_2), а $\tilde{A}_{u,w}$ кодирует (σ_3, σ_4), причем $\sigma_1 \neq \sigma_3$, то

$$\Pr_{r,h}[\tilde{A}_{u,w}(r_1 + h) \neq \tilde{B}_u(r) + \tilde{A}_{u,w}(h)] \geqslant \frac{1}{2} \qquad (*)$$

(выполняется при $r(\sigma_1) \neq r(\sigma_3)$).

Лемма о согласовании

Для любого хорошего ребра (u, w), где $\tilde{B}_u$ кодирует σ_1, а $\tilde{B}_w$ кодирует σ_2, $\tilde{A}_{u,w}$ кодирует пару (σ_1, σ_2).

Согласование в вершинах

По определению, $\tilde{B}_u(r) = \tilde{A}_{u,v}(r_1)$.
Если $\tilde{A}_{u,v}$ является кодом пары (σ_1, σ_2), то $\tilde{B}_u$ является кодом σ_1.
Отсюда получаем: если $\tilde{A}_{u,v}$ кодирует (σ_1, σ_2), а $\tilde{A}_{u,w}$ кодирует (σ_3, σ_4), причем $\sigma_1 \neq \sigma_3$, то

$$\mathop{\mathbf{Pr}}_{r,h}[\tilde{A}_{u,w}(r_1 + h) \neq \tilde{B}_u(r) + \tilde{A}_{u,w}(h)] \geqslant \frac{1}{2} \qquad (*)$$

(выполняется при $r(\sigma_1) \neq r(\sigma_3)$).

Лемма о согласовании

Для любого хорошего ребра (u, w), где $\tilde{B}_u$ кодирует σ_1, а $\tilde{B}_w$ кодирует σ_2, $\tilde{A}_{u,w}$ кодирует пару (σ_1, σ_2).

Согласование в вершинах

По определению, $\tilde{B}_u(r) = \tilde{A}_{u,v}(r_1)$.
Если $\tilde{A}_{u,v}$ является кодом пары (σ_1, σ_2), то $\tilde{B}_u$ является кодом σ_1.
Отсюда получаем: если $\tilde{A}_{u,v}$ кодирует (σ_1, σ_2), а $\tilde{A}_{u,w}$ кодирует (σ_3, σ_4), причем $\sigma_1 \neq \sigma_3$, то

$$\mathop{\mathbf{Pr}}_{r,h}[\tilde{A}_{u,w}(r_1 + h) \neq \tilde{B}_u(r) + \tilde{A}_{u,w}(h)] \geqslant \frac{1}{2} \qquad (*)$$

(выполняется при $r(\sigma_1) \neq r(\sigma_3)$).

Лемма о согласовании

Для любого хорошего ребра (u, w), где $\tilde{B}_u$ кодирует σ_1, а $\tilde{B}_w$ кодирует σ_2, $\tilde{A}_{u,w}$ кодирует пару (σ_1, σ_2).

Доказательство леммы о согласовании

Если (u, w) — хорошее, то $\tilde{B}_u(r) = \tilde{A}_{u,v}(r_1)$ для хорошего (u, v).

Учитывая линейность, получаем аналогично предыдущему

$$\Pr_r[\tilde{B}_u(r) \neq B_u(r)] = \Pr_r[\tilde{A}_{u,v}(r_1) \neq B_u(r)] =$$
$$= \Pr_{r,h}[\tilde{A}_{u,v}(r_1 + h) \neq B_u(r) + \tilde{A}_{u,v}(h)] < \frac{1}{20} + \frac{1}{20} + \frac{1}{22} < \frac{3}{20}\,.$$

Далее

$$\Pr_{r,h}[\tilde{A}_{u,w}(r_1 + h) \neq \tilde{B}_u(r) + \tilde{A}_{u,w}(h)] \leqslant$$
$$\leqslant \Pr_{r,h}[\tilde{A}_{u,w}(r_1 + h) \neq B_u(r) + \tilde{A}_{u,w}(h)] + \Pr_r[\tilde{B}_u(r) \neq B_u(r)] <$$
$$< \left(\frac{1}{20} + \frac{1}{20} + \frac{1}{22}\right) + \frac{3}{20} < \frac{3}{10}\,.$$

Из $(*)$ видим, что $\tilde{A}_{u,w}$ кодирует пару (σ_1, σ_4), где $\tilde{B}_u$ кодирует σ_1.
Аналогично проверяется согласование во вторых компонентах пар.

Доказательство леммы о согласовании

Если (u, w) — хорошее, то $\tilde{B}_u(r) = \tilde{A}_{u,v}(r_1)$ для хорошего (u, v).
Учитывая линейность, получаем аналогично предыдущему

$$\Pr_r[\tilde{B}_u(r) \neq B_u(r)] = \Pr_r[\tilde{A}_{u,v}(r_1) \neq B_u(r)] =$$

$$= \Pr_{r,h}[\tilde{A}_{u,v}(r_1 + h) \neq B_u(r) + \tilde{A}_{u,v}(h)] < \frac{1}{20} + \frac{1}{20} + \frac{1}{22} < \frac{3}{20}\,.$$

Далее

$$\Pr_{r,h}[\tilde{A}_{u,w}(r_1 + h) \neq \tilde{B}_u(r) + \tilde{A}_{u,w}(h)] \leqslant$$

$$\leqslant \Pr_{r,h}[\tilde{A}_{u,w}(r_1 + h) \neq B_u(r) + \tilde{A}_{u,w}(h)] + \Pr_r[\tilde{B}_u(r) \neq B_u(r)] <$$

$$< \left(\frac{1}{20} + \frac{1}{20} + \frac{1}{22}\right) + \frac{3}{20} < \frac{3}{10}\,.$$

Из $(*)$ видим, что $\tilde{A}_{u,w}$ кодирует пару (σ_1, σ_4), где $\tilde{B}_u$ кодирует σ_1.
Аналогично проверяется согласование во вторых компонентах пар.

Доказательство леммы о согласовании

Если (u, w) — хорошее, то $\tilde{B}_u(r) = \tilde{A}_{u,v}(r_1)$ для хорошего (u, v).
Учитывая линейность, получаем аналогично предыдущему

$$\Pr_r[\tilde{B}_u(r) \neq B_u(r)] = \Pr_r[\tilde{A}_{u,v}(r_1) \neq B_u(r)] =$$
$$= \Pr_{r,h}[\tilde{A}_{u,v}(r_1 + h) \neq B_u(r) + \tilde{A}_{u,v}(h)] < \frac{1}{20} + \frac{1}{20} + \frac{1}{22} < \frac{3}{20}\,.$$

Далее

$$\Pr_{r,h}[\tilde{A}_{u,w}(r_1 + h) \neq \tilde{B}_u(r) + \tilde{A}_{u,w}(h)] \leqslant$$
$$\leqslant \Pr_{r,h}[\tilde{A}_{u,w}(r_1 + h) \neq B_u(r) + \tilde{A}_{u,w}(h)] + \Pr_r[\tilde{B}_u(r) \neq B_u(r)] <$$
$$< \left(\frac{1}{20} + \frac{1}{20} + \frac{1}{22}\right) + \frac{3}{20} < \frac{3}{10}\,.$$

Из $(*)$ видим, что $\tilde{A}_{u,w}$ кодирует пару (σ_1, σ_4), где $\tilde{B}_u$ кодирует σ_1.
Аналогично проверяется согласование во вторых компонентах пар.

Доказательство леммы о согласовании

Если (u, w) — хорошее, то $\tilde{B}_u(r) = \tilde{A}_{u,v}(r_1)$ для хорошего (u, v). Учитывая линейность, получаем аналогично предыдущему

$$\Pr_r[\tilde{B}_u(r) \neq B_u(r)] = \Pr_r[\tilde{A}_{u,v}(r_1) \neq B_u(r)] =$$
$$= \Pr_{r,h}[\tilde{A}_{u,v}(r_1 + h) \neq B_u(r) + \tilde{A}_{u,v}(h)] < \frac{1}{20} + \frac{1}{20} + \frac{1}{22} < \frac{3}{20}.$$

Далее

$$\Pr_{r,h}[\tilde{A}_{u,w}(r_1 + h) \neq \tilde{B}_u(r) + \tilde{A}_{u,w}(h)] \leqslant$$
$$\leqslant \Pr_{r,h}[\tilde{A}_{u,w}(r_1 + h) \neq B_u(r) + \tilde{A}_{u,w}(h)] + \Pr_r[\tilde{B}_u(r) \neq B_u(r)] <$$
$$< \left(\frac{1}{20} + \frac{1}{20} + \frac{1}{22}\right) + \frac{3}{20} < \frac{3}{10}.$$

Из $(*)$ видим, что $\tilde{A}_{u,w}$ кодирует пару (σ_1, σ_4), где $\tilde{B}_u$ кодирует σ_1. Аналогично проверяется согласование во вторых компонентах пар.

Выполнение ограничения

Утверждение

Если (u, v) — хорошее и $A_{u,v} = L(\sigma_1, \sigma_2)$, то для пары (σ_1, σ_2) выполнено ограничение на ребре (u, v) графа G.

Из леммы о близости получаем

$$\Pr_h[\tilde{A}_{u,v}(c(u,v)+h) \neq 1 + \tilde{A}_{u,v}(h)] <$$
$$< \Pr_h[A_{u,v}(c(u,v)+h) \neq 1 + A_{u,v}(h)] + \frac{1}{20} + \frac{1}{20} < \frac{3}{20}.$$

Значит, для некоторого h'

$$\tilde{A}_{u,v}(c(u,v)+h') = \tilde{A}_{u,v}(c(u,v)) + \tilde{A}_{u,v}(h') = 1 + \tilde{A}_{u,v}(h').$$

То есть $\tilde{A}_{u,v}(c(u,v)) = 1$, это и означает выполнение ограничения на паре (σ_1, σ_2).

Выполнение ограничения

Утверждение

Если (u, v) — хорошее и $A_{u,v} = L(\sigma_1, \sigma_2)$, то для пары (σ_1, σ_2) выполнено ограничение на ребре (u, v) графа G.

Из леммы о близости получаем

$$\Pr_h[\tilde{A}_{u,v}(c(u, v) + h) \neq 1 + \tilde{A}_{u,v}(h)] <$$
$$< \Pr_h[A_{u,v}(c(u, v) + h) \neq 1 + A_{u,v}(h)] + \frac{1}{20} + \frac{1}{20} < \frac{3}{20}\,.$$

Значит, для некоторого h'

$$\tilde{A}_{u,v}(c(u, v) + h') = \tilde{A}_{u,v}(c(u, v)) + \tilde{A}_{u,v}(h') = 1 + \tilde{A}_{u,v}(h').$$

То есть $\tilde{A}_{u,v}(c(u, v)) = 1$, это и означает выполнение ограничения на паре (σ_1, σ_2).

Выполнение ограничения

Утверждение

Если (u, v) — хорошее и $A_{u,v} = L(\sigma_1, \sigma_2)$, то для пары (σ_1, σ_2) выполнено ограничение на ребре (u, v) графа G.

Из леммы о близости получаем

$$\Pr_h[\tilde{A}_{u,v}(c(u,v)+h) \neq 1 + \tilde{A}_{u,v}(h)] <$$

$$< \Pr_h[A_{u,v}(c(u,v)+h) \neq 1 + A_{u,v}(h)] + \frac{1}{20} + \frac{1}{20} < \frac{3}{20}\,.$$

Значит, для некоторого h'

$$\tilde{A}_{u,v}(c(u,v)+h') = \tilde{A}_{u,v}(c(u,v)) + \tilde{A}_{u,v}(h') = 1 + \tilde{A}_{u,v}(h').$$

То есть $\tilde{A}_{u,v}(c(u,v)) = 1$, это и означает выполнение ограничения на паре (σ_1, σ_2).

Выполнение ограничения

Утверждение

Если (u,v) — хорошее и $A_{u,v} = L(\sigma_1, \sigma_2)$, то для пары (σ_1, σ_2) выполнено ограничение на ребре (u,v) графа G.

Из леммы о близости получаем

$$\Pr_h[\tilde{A}_{u,v}(c(u,v)+h) \neq 1 + \tilde{A}_{u,v}(h)] <$$
$$< \Pr_h[A_{u,v}(c(u,v)+h) \neq 1 + A_{u,v}(h)] + \frac{1}{20} + \frac{1}{20} < \frac{3}{20}\,.$$

Значит, для некоторого h'

$$\tilde{A}_{u,v}(c(u,v)+h') = \tilde{A}_{u,v}(c(u,v)) + \tilde{A}_{u,v}(h') = 1 + \tilde{A}_{u,v}(h').$$

То есть $\tilde{A}_{u,v}(c(u,v)) = 1$, это и означает выполнение ограничения на паре (σ_1, σ_2).

Собираем вместе

По присваиванию $(A_{u,v}, B_u)$ мы построили присваивание $(\tilde{A}_{u,v}, \tilde{B}_u)$, которое на хороших ребрах

- кодирует пары символов (σ_1, σ_2);
- для этих пар символов выполнено ограничение исходного графа ограничений на ребре (u, v);
- $\tilde{B}_u$ кодирует символы, отвечающие концу любого хорошего ребра, инцидентного u.

Доказательство основной леммы

Зазадим присваивание σ в соответствии с кодами $\tilde{B}_u$ (в вершинах, которые неинцидентны ни одному хорошему ребру, выбираем значение произвольно).

Присваивание σ выполняет ограничения на всех хороших ребрах.

Доля плохих ребер не больше 22δ. Поэтому

$$\frac{1}{22}\mathrm{UNSAT}(G) \leqslant \frac{1}{22}\mathrm{UNSAT}_\sigma(G) \leqslant \mathrm{UNSAT}_{\sigma'}(H).$$

Собираем вместе

По присваиванию $(A_{u,v}, B_u)$ мы построили присваивание $(\tilde{A}_{u,v}, \tilde{B}_u)$, которое на хороших ребрах

- кодирует пары символов (σ_1, σ_2);
- для этих пар символов выполнено ограничение исходного графа ограничений на ребре (u, v);
- $\tilde{B}_u$ кодирует символы, отвечающие концу любого хорошего ребра, инцидентного u.

Доказательство основной леммы

Зазадим присваивание σ в соответствии с кодами $\tilde{B}_u$ (в вершинах, которые неинцидентны ни одному хорошему ребру, выбираем значение произвольно).

Присваивание σ выполняет ограничения на всех хороших ребрах.

Доля плохих ребер не больше 22δ. Поэтому

$$\frac{1}{22}\mathrm{UNSAT}(G) \leqslant \frac{1}{22}\mathrm{UNSAT}_{\sigma}(G) \leqslant \mathrm{UNSAT}_{\sigma'}(H).$$

Собираем вместе

По присваиванию $(A_{u,v}, B_u)$ мы построили присваивание $(\tilde{A}_{u,v}, \tilde{B}_u)$, которое на хороших ребрах

- кодирует пары символов (σ_1, σ_2);
- для этих пар символов выполнено ограничение исходного графа ограничений на ребре (u, v);
- $\tilde{B}_u$ кодирует символы, отвечающие концу любого хорошего ребра, инцидентного u.

Доказательство основной леммы

Зададим присваивание σ в соответствии с кодами $\tilde{B}_u$ (в вершинах, которые неинцидентны ни одному хорошему ребру, выбираем значение произвольно).

Присваивание σ выполняет ограничения на всех хороших ребрах.

Доля плохих ребер не больше 22δ. Поэтому

$$\frac{1}{22}\mathrm{UNSAT}(G) \leqslant \frac{1}{22}\mathrm{UNSAT}_\sigma(G) \leqslant \mathrm{UNSAT}_{\sigma'}(H).$$

Собираем вместе

По присваиванию $(A_{u,v}, B_u)$ мы построили присваивание $(\tilde{A}_{u,v}, \tilde{B}_u)$, которое на хороших ребрах

- кодирует пары символов (σ_1, σ_2);
- для этих пар символов выполнено ограничение исходного графа ограничений на ребре (u, v);
- $\tilde{B}_u$ кодирует символы, отвечающие концу любого хорошего ребра, инцидентного u.

Доказательство основной леммы

Зазадим присваивание σ в соответствии с кодами $\tilde{B}_u$ (в вершинах, которые неинцидентны ни одному хорошему ребру, выбираем значение произвольно).

Присваивание σ выполняет ограничения на всех хороших ребрах.

Доля плохих ребер не больше 22δ. Поэтому

$$\frac{1}{22}\mathrm{UNSAT}(G) \leqslant \frac{1}{22}\mathrm{UNSAT}_{\sigma}(G) \leqslant \mathrm{UNSAT}_{\sigma'}(H).$$

План

1 Увеличение зазора

2 Уменьшение алфавита: локально проверяемые коды

3 Преобразование k-выполнимости в 2-выполнимость

4 Улучшение графа

5 Выбор параметров

Преобразование в 2-выполнимость

Пусть $G(V, E, \{0,1\}, c)$ — k-арный гиперграф. Преобразуем его в обычный ($k = 2$) двудольный граф G' с алфавитом $\{0,1\}^k$.

Вершины G': вершины и рёбра G.

Рёбра G': инцидентные пары (вершина $v \in V(G)$, ребро $e \in E(G)$).

Обозначение вершин G': $\hat{v}$, $\hat{e}$.

Ограничения: пусть v входит в e на месте j. Тогда ограничение на ребре $(\hat{x}, \hat{e})$ выполнено при присваивании $\sigma' \colon V(G') \to \{0,1\}^k$ тогда и только тогда, когда $\sigma'(\hat{e})$ выполняет ограничение на ребре e исходного графа и

$$\sigma'(\hat{e})(j) = \sigma'(\hat{v})(1).$$

Каждому ребру исходного гиперграфа G отвечает k ребер графа G'.

Преобразование в 2-выполнимость

Пусть $G(V, E, \{0,1\}, c)$ — k-арный гиперграф. Преобразуем его в обычный ($k = 2$) двудольный граф G' с алфавитом $\{0,1\}^k$.
Вершины G': вершины и рёбра G.
Рёбра G': инцидентные пары (вершина $v \in V(G)$, ребро $e \in E(G)$).
Обозначение вершин G': $\hat{v}$, $\hat{e}$.
Ограничения: пусть v входит в e на месте j. Тогда ограничение на ребре $(\hat{x}, \hat{e})$ выполнено при присваивании $\sigma' \colon V(G') \to \{0,1\}^k$ тогда и только тогда, когда $\sigma'(\hat{e})$ выполняет ограничение на ребре e исходного графа и

$$\sigma'(\hat{e})(j) = \sigma'(\hat{v})(1).$$

Каждому ребру исходного гиперграфа G отвечает k ребер графа G'.

Преобразование в 2-выполнимость

Пусть $G(V, E, \{0,1\}, c)$ — k-арный гиперграф. Преобразуем его в обычный ($k = 2$) двудольный граф G' с алфавитом $\{0,1\}^k$.

Вершины G': вершины и рёбра G.

Рёбра G': инцидентные пары (вершина $v \in V(G)$, ребро $e \in E(G)$).

Обозначение вершин G': $\hat{v}$, $\hat{e}$.

Ограничения: пусть v входит в e на месте j. Тогда ограничение на ребре $(\hat{x}, \hat{e})$ выполнено при присваивании $\sigma' \colon V(G') \to \{0,1\}^k$ тогда и только тогда, когда $\sigma'(\hat{e})$ выполняет ограничение на ребре e исходного графа и

$$\sigma'(\hat{e})(j) = \sigma'(\hat{v})(1).$$

Каждому ребру исходного гиперграфа G отвечает k ребер графа G'.

Преобразование в 2-выполнимость

Пусть $G(V, E, \{0,1\}, c)$ — k-арный гиперграф. Преобразуем его в обычный ($k = 2$) двудольный граф G' с алфавитом $\{0,1\}^k$.
Вершины G': вершины и рёбра G.
Рёбра G': инцидентные пары (вершина $v \in V(G)$, ребро $e \in E(G)$).
Обозначение вершин G': $\hat{v}$, $\hat{e}$.
Ограничения: пусть v входит в e на месте j. Тогда ограничение на ребре $(\hat{x}, \hat{e})$ выполнено при присваивании $\sigma' \colon V(G') \to \{0,1\}^k$ тогда и только тогда, когда $\sigma'(\hat{e})$ выполняет ограничение на ребре e исходного графа и

$$\sigma'(\hat{e})(j) = \sigma'(\hat{v})(1).$$

Каждому ребру исходного гиперграфа G отвечает k ребер графа G'.

Преобразование в 2-выполнимость

Пусть $G(V, E, \{0,1\}, c)$ — k-арный гиперграф. Преобразуем его в обычный ($k = 2$) двудольный граф G' с алфавитом $\{0,1\}^k$.

Вершины G': вершины и рёбра G.

Рёбра G': инцидентные пары (вершина $v \in V(G)$, ребро $e \in E(G)$).

Обозначение вершин G': $\hat{v}$, $\hat{e}$.

Ограничения: пусть v входит в e на месте j. Тогда ограничение на ребре $(\hat{x}, \hat{e})$ выполнено при присваивании $\sigma' \colon V(G') \to \{0,1\}^k$ тогда и только тогда, когда $\sigma'(\hat{e})$ выполняет ограничение на ребре e исходного графа и

$$\sigma'(\hat{e})(j) = \sigma'(\hat{v})(1).$$

Каждому ребру исходного гиперграфа G отвечает k ребер графа G'.

Оценка зазора

Лемма

$\mathrm{UNSAT}(G) = \mathrm{UNSAT}(G')$.

Неравенство в одну сторону (σ оптимально для G):

1. Полагаем $\sigma'(\hat{v})(1) = \sigma(v)$, $\sigma'(\hat{e}) = (\sigma(v_1), \ldots, \sigma(v_k))$.
2. Общее количество нарушений в σ' в k раз больше, чем в σ. Доля та же. Т. е. $\mathrm{UNSAT}(G') \leqslant \mathrm{UNSAT}_{\sigma'}(G') = \mathrm{UNSAT}_{\sigma}(G) = \mathrm{UNSAT}(G)$.

Неравенство в другую сторону (σ' оптимально для G'):

1. Полагаем $\sigma(v) = \sigma'(\hat{v})(1)$.
2. Каждое нарушение в σ дает k нарушений в σ' (и могут быть еще).
3. Количество ребер тоже изменяется в k раз. Значит, $\mathrm{UNSAT}(G') = \mathrm{UNSAT}_{\sigma'}(G') \geqslant \mathrm{UNSAT}_{\sigma}(G) \geqslant \mathrm{UNSAT}(G)$.

Оценка зазора

Лемма

$\mathrm{UNSAT}(G) = \mathrm{UNSAT}(G')$.

Неравенство в одну сторону (σ оптимально для G):

1. Полагаем $\sigma'(\hat{v})(1) = \sigma(v)$, $\sigma'(\hat{e}) = (\sigma(v_1), \ldots, \sigma(v_k))$.
2. Общее количество нарушений в σ' в k раз больше, чем в σ. Доля та же. Т. е. $\mathrm{UNSAT}(G') \leqslant \mathrm{UNSAT}_{\sigma'}(G') = \mathrm{UNSAT}_{\sigma}(G) = \mathrm{UNSAT}(G)$.

Неравенство в другую сторону (σ' оптимально для G'):

1. Полагаем $\sigma(v) = \sigma'(\hat{v})(1)$.
2. Каждое нарушение в σ дает k нарушений в σ' (и могут быть еще).
3. Количество ребер тоже изменяется в k раз. Значит, $\mathrm{UNSAT}(G') = \mathrm{UNSAT}_{\sigma'}(G') \geqslant \mathrm{UNSAT}_{\sigma}(G) \geqslant \mathrm{UNSAT}(G)$.

Оценка зазора

Лемма

$\mathrm{UNSAT}(G) = \mathrm{UNSAT}(G')$.

Неравенство в одну сторону (σ оптимально для G):

1. Полагаем $\sigma'(\hat{v})(1) = \sigma(v)$, $\sigma'(\hat{e}) = (\sigma(v_1), \ldots, \sigma(v_k))$.
2. Общее количество нарушений в σ' в k раз больше, чем в σ. Доля та же. Т. е. $\mathrm{UNSAT}(G') \leqslant \mathrm{UNSAT}_{\sigma'}(G') = \mathrm{UNSAT}_{\sigma}(G) = \mathrm{UNSAT}(G)$.

Неравенство в другую сторону (σ' оптимально для G'):

1. Полагаем $\sigma(v) = \sigma'(\hat{v})(1)$.
2. Каждое нарушение в σ дает k нарушений в σ' (и могут быть еще).
3. Количество ребер тоже изменяется в k раз. Значит, $\mathrm{UNSAT}(G') = \mathrm{UNSAT}_{\sigma'}(G') \geq \mathrm{UNSAT}_{\sigma}(G) \geq \mathrm{UNSAT}(G)$.

Оценка зазора

Лемма

$\textsc{unsat}(G) = \textsc{unsat}(G')$.

Неравенство в одну сторону (σ оптимально для G):

1. Полагаем $\sigma'(\hat{v})(1) = \sigma(v)$, $\sigma'(\hat{e}) = (\sigma(v_1), \ldots, \sigma(v_k))$.
2. Общее количество нарушений в σ' в k раз больше, чем в σ. Доля та же. Т. е. $\textsc{unsat}(G') \leqslant \textsc{unsat}_{\sigma'}(G') = \textsc{unsat}_{\sigma}(G) = \textsc{unsat}(G)$.

Неравенство в другую сторону (σ' оптимально для G'):

1. Полагаем $\sigma(v) = \sigma'(\hat{v})(1)$.
2. Каждое нарушение в σ дает k нарушений в σ' (и могут быть еще).
3. Количество ребер тоже изменяется в k раз. Значит, $\textsc{unsat}(G') = \textsc{unsat}_{\sigma'}(G') \geqslant \textsc{unsat}_{\sigma}(G) \geqslant \textsc{unsat}(G)$.

Оценка зазора

Лемма

$\text{UNSAT}(G) = \text{UNSAT}(G')$.

Неравенство в одну сторону (σ оптимально для G):

1. Полагаем $\sigma'(\hat{v})(1) = \sigma(v)$, $\sigma'(\hat{e}) = (\sigma(v_1), \dots, \sigma(v_k))$.
2. Общее количество нарушений в σ' в k раз больше, чем в σ. Доля та же. Т. е. $\text{UNSAT}(G') \leqslant \text{UNSAT}_{\sigma'}(G') = \text{UNSAT}_{\sigma}(G) = \text{UNSAT}(G)$.

Неравенство в другую сторону (σ' оптимально для G'):

1. Полагаем $\sigma(v) = \sigma'(\hat{v})(1)$.
2. Каждое нарушение в σ дает k нарушений в σ' (и могут быть еще).
3. Количество ребер тоже изменяется в k раз. Значит, $\text{UNSAT}(G') = \text{UNSAT}_{\sigma'}(G') \geqslant \text{UNSAT}_{\sigma}(G) \geqslant \text{UNSAT}(G)$.

Оценка зазора

Лемма

$\mathrm{UNSAT}(G) = \mathrm{UNSAT}(G')$.

Неравенство в одну сторону (σ оптимально для G):

1. Полагаем $\sigma'(\hat{v})(1) = \sigma(v)$, $\sigma'(\hat{e}) = (\sigma(v_1), \ldots, \sigma(v_k))$.
2. Общее количество нарушений в σ' в k раз больше, чем в σ. Доля та же. Т. е. $\mathrm{UNSAT}(G') \leqslant \mathrm{UNSAT}_{\sigma'}(G') = \mathrm{UNSAT}_{\sigma}(G) = \mathrm{UNSAT}(G)$.

Неравенство в другую сторону (σ' оптимально для G'):

1. Полагаем $\sigma(v) = \sigma'(\hat{v})(1)$.
2. Каждое нарушение в σ дает k нарушений в σ' (и могут быть еще).
3. Количество ребер тоже изменяется в k раз. Значит, $\mathrm{UNSAT}(G') = \mathrm{UNSAT}_{\sigma'}(G') \geqslant \mathrm{UNSAT}_{\sigma}(G) \geqslant \mathrm{UNSAT}(G)$.

План

1 Увеличение зазора

2 Уменьшение алфавита: локально проверяемые коды

3 Преобразование k-выполнимости в 2-выполнимость

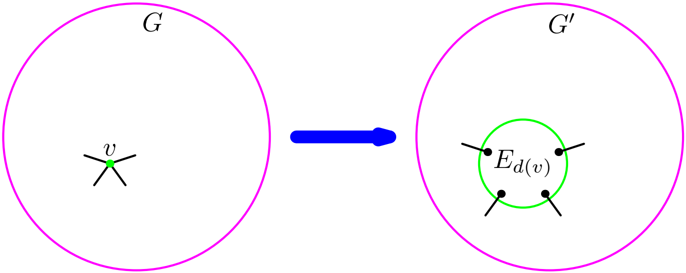
4 Улучшение графа

5 Выбор параметров

Произвольный граф ограничений в регулярный

Вместо вершины v степени d вклеиваем экспандер степени d_0 на $d(v)$ вершинах с коэффициентом реберного расширения h_0.
Ограничения на новых ребрах: равенства значений в концах ребра. На старых ребрах ограничения сохраняются.

$\Sigma' = \Sigma$

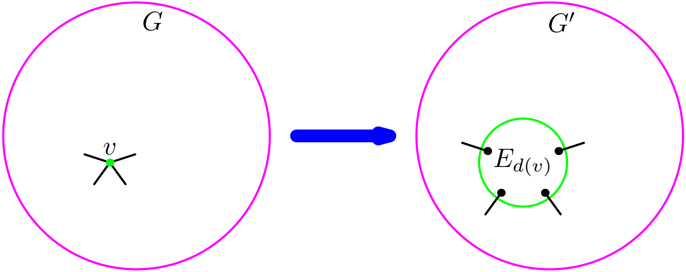


1. Граф G' — регулярный степени $d = d_0 + 1$.
2. Размер графа увеличивается линейно (количество ребер увеличивается в d раз).

Произвольный граф ограничений в регулярный

Вместо вершины v степени d вклеиваем экспандер степени d_0 на $d(v)$ вершинах с коэффициентом реберного расширения h_0.
Ограничения на новых ребрах: равенства значений в концах ребра. На старых ребрах ограничения сохраняются.

$\Sigma' = \Sigma$

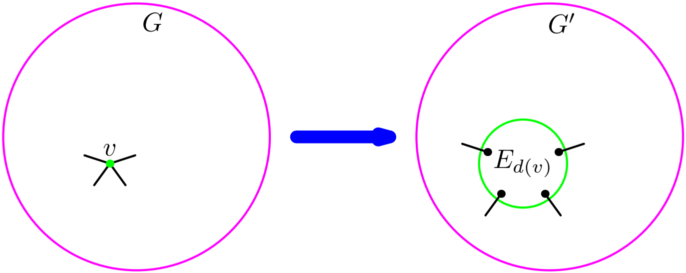


1. Граф G' — регулярный степени $d = d_0 + 1$.
2. Размер графа увеличивается линейно (количество ребер увеличивается в d раз).

Произвольный граф ограничений в регулярный

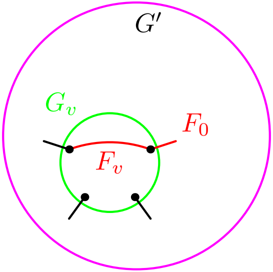
Вместо вершины v степени d вклеиваем экспандер степени d_0 на $d(v)$ вершинах с коэффициентом реберного расширения h_0.
Ограничения на новых ребрах: равенства значений в концах ребра. На старых ребрах ограничения сохраняются.

$$\Sigma' = \Sigma$$



1. Граф G' — регулярный степени $d = d_0 + 1$.
2. Размер графа увеличивается линейно (количество ребер увеличивается в d раз).

Оценка зазора



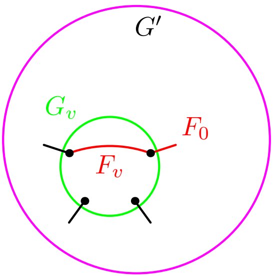
Пусть σ' — присваивание в G', которое нарушает ограничения на множестве ребер $F' = F_0 \cup \bigcup_{v \in V} F_v$.

Определим присваивание в G голосованием по большинству:

$$\sigma(v) = \arg\max_{\sigma} \left| \{ v' \in G_v \mid \sigma'(v') = \sigma \} \right|.$$

Пусть σ нарушает ограничения на множестве ребер F.

Оценка зазора



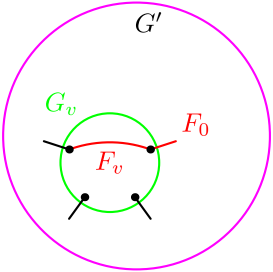
Пусть σ' — присваивание в G', которое нарушает ограничения на множестве ребер $F' = F_0 \cup \bigcup_{v \in V} F_v$.

Определим присваивание в G голосованием по большинству:

$$\sigma(v) = \arg\max_{\sigma} \left| \{ v' \in G_v \mid \sigma'(v') = \sigma \} \right|.$$

Пусть σ нарушает ограничения на множестве ребер F.

Оценка зазора (2)



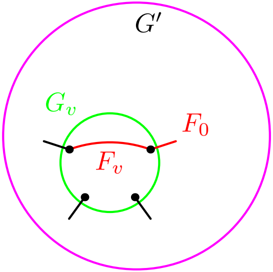
$$\delta' = \mathrm{UNSAT}_{\sigma'}(G') = F'/E' = F'/(dE)$$
$$\delta = \mathrm{UNSAT}_{\sigma}(G) = F/E$$
$$S_v = \{x \in G_v \mid \sigma'(x) \neq \sigma(v)\}$$
$$S = \bigcup_v S_v$$

Для каждого ребра из F или нарушается ограничение присваиванием σ', или один из концов принадлежит S:

$$F' + S \geqslant F_0 + S \geqslant F = \delta E.$$

Если $F' \geqslant \frac{\delta}{2}E$, то $\delta' \geqslant \frac{\delta}{2d}$. В противном случае $S \geqslant \frac{\delta}{2}E$.

Оценка зазора (2)



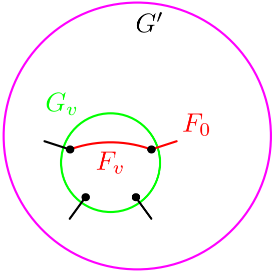
$$\delta' = \mathrm{UNSAT}_{\sigma'}(G') = F'/E' = F'/(dE)$$
$$\delta = \mathrm{UNSAT}_{\sigma}(G) = F/E$$
$$S_v = \{x \in G_v \mid \sigma'(x) \neq \sigma(v)\}$$
$$S = \bigcup_v S_v$$

Для каждого ребра из F или нарушается ограничение присваиванием σ', или один из концов принадлежит S:

$$F' + S \geqslant F_0 + S \geqslant F = \delta E.$$

Если $F' \geqslant \dfrac{\delta}{2}E$, то $\delta' \geqslant \dfrac{\delta}{2d}$. В противном случае $S \geqslant \dfrac{\delta}{2}E$.

Оценка зазора (2)



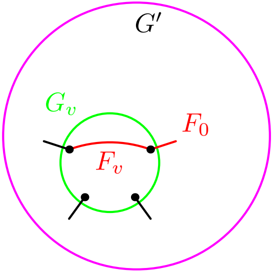
$$\delta' = \mathrm{UNSAT}_{\sigma'}(G') = F'/E' = F'/(dE)$$
$$\delta = \mathrm{UNSAT}_{\sigma}(G) = F/E$$
$$S_v = \{x \in G_v \mid \sigma'(x) \neq \sigma(v)\}$$
$$S = \bigcup_v S_v$$

Для каждого ребра из F или нарушается ограничение присваиванием σ', или один из концов принадлежит S:

$$F' + S \geqslant F_0 + S \geqslant F = \delta E.$$

Если $F' \geqslant \frac{\delta}{2}E$, то $\delta' \geqslant \frac{\delta}{2d}$. В противном случае $S \geqslant \frac{\delta}{2}E$.

Оценка зазора (2)



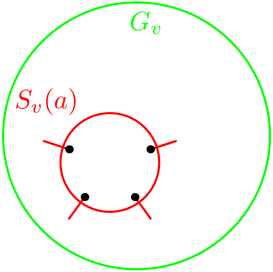
$\delta' = \mathrm{UNSAT}_{\sigma'}(G') = F'/E' = F'/(dE)$
$\delta = \mathrm{UNSAT}_{\sigma}(G) = F/E$
$S_v = \{x \in G_v \mid \sigma'(x) \neq \sigma(v)\}$
$S = \bigcup_v S_v$

Для каждого ребра из F или нарушается ограничение присваиванием σ', или один из концов принадлежит S:

$$F' + S \geqslant F_0 + S \geqslant F = \delta E.$$

Если $F' \geqslant \frac{\delta}{2}E$, то $\delta' \geqslant \frac{\delta}{2d}$. В противном случае $S \geqslant \frac{\delta}{2}E$.

Оценка зазора (3)



$S \geqslant \frac{\delta}{2} E$

$S_v(a) = \{x \in G_v \mid \sigma'(x) = a\}$

$a \neq \sigma(v) \quad \Rightarrow \quad |S_v(a)| \leqslant |V(G_v)|/2$

В G_v имеем $E(S_v(a), \bar{S}_v(a)) \geqslant h_0 |S_v(a)|$

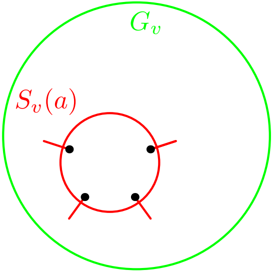
$F_v \geqslant \frac{h_0}{2} |S_v|$

$$\delta' = \frac{F'}{E'} \geqslant \frac{\sum_v F_v}{dE} \geqslant \frac{h_0}{2d} \cdot \frac{S}{E} \geqslant \frac{h_0}{4d} \delta.$$

Лемма

Для преобразования вклейки экспандеров выполняется

$$\min\left(\frac{1}{2d}, \frac{h_0}{4d}\right) \mathrm{UNSAT}(G) \leqslant \mathrm{UNSAT}(G') \leqslant \mathrm{UNSAT}(G).$$



$$S \geqslant \frac{\delta}{2} E$$

$$S_v(a) = \{x \in G_v \mid \sigma'(x) = a\}$$

$$a \neq \sigma(v) \quad \Rightarrow \quad |S_v(a)| \leqslant |V(G_v)|/2$$

В G_v имеем $E(S_v(a), \bar{S}_v(a)) \geqslant h_0 |S_v(a)|$

$$F_v \geqslant \frac{h_0}{2} |S_v|$$

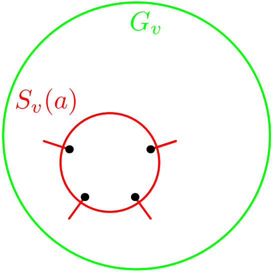
$$\delta' = \frac{F'}{E'} \geqslant \frac{\sum_v F_v}{dE} \geqslant \frac{h_0}{2d} \cdot \frac{S}{E} \geqslant \frac{h_0}{4d} \delta.$$

Лемма

Для преобразования вклейки экспандеров выполняется

$$\min\left(\frac{1}{2d}, \frac{h_0}{4d}\right) \mathrm{UNSAT}(G) \leqslant \mathrm{UNSAT}(G') \leqslant \mathrm{UNSAT}(G).$$

Оценка зазора (3)



$$S \geqslant \frac{\delta}{2} E$$

$$S_v(a) = \{x \in G_v \mid \sigma'(x) = a\}$$

$$a \neq \sigma(v) \quad \Rightarrow \quad |S_v(a)| \leqslant |V(G_v)|/2$$

В G_v имеем $E(S_v(a), \bar{S}_v(a)) \geqslant h_0 |S_v(a)|$

$$F_v \geqslant \frac{h_0}{2} |S_v|$$

$$\delta' = \frac{F'}{E'} \geqslant \frac{\sum_v F_v}{dE} \geqslant \frac{h_0}{2d} \cdot \frac{S}{E} \geqslant \frac{h_0}{4d} \delta.$$

Лемма

Для преобразования вклейки экспандеров выполняется

$$\min\left(\frac{1}{2d}, \frac{h_0}{4d}\right) \text{UNSAT}(G) \leqslant \text{UNSAT}(G') \leqslant \text{UNSAT}(G).$$

Регулярный граф в экспандер с малой потерей в зазоре

- Добавляем к d-регулярному графу G рёбра d_0-экспандера на том же множестве вершин.
- Добавляем к каждой вершине $d + d_0$ петель.
- На добавленных ребрах ограничения всегда выполнены.
- Увеличение размера графа линейное.

Теорема о реберных и алгебраических экспандерах

$$1 - 2\frac{h(G)}{d} \leqslant \frac{\lambda(G)}{d} \leqslant 1 - \frac{h(G)^2}{2d^2}$$

Лемма об экспандеризации

Существует полиномиально вычислимое преобразование $G \mapsto G''$, которое любой граф ограничений переводит в (λ, d'')-экспандер с $\lambda < 1$, размер графа ограничений увеличивается линейно, а

$$\beta_1 \text{UNSAT}(G) \leqslant \text{UNSAT}(G'') \leqslant \text{UNSAT}(G).$$

Регулярный граф в экспандер с малой потерей в зазоре

- Добавляем к d-регулярному графу G рёбра d_0-экспандера на том же множестве вершин.
- Добавляем к каждой вершине $d + d_0$ петель.
- На добавленных ребрах ограничения всегда выполнены.
- Увеличение размера графа линейное.

Теорема о реберных и алгебраических экспандерах

$$1 - 2\frac{h(G)}{d} \leqslant \frac{\lambda(G)}{d} \leqslant 1 - \frac{h(G)^2}{2d^2}$$

Лемма об экспандеризации

Существует полиномиально вычислимое преобразование $G \mapsto G''$, которое любой граф ограничений переводит в (λ, d'')-экспандер с $\lambda < 1$, размер графа ограничений увеличивается линейно, а

$$\beta_1 \text{UNSAT}(G) \leqslant \text{UNSAT}(G'') \leqslant \text{UNSAT}(G).$$

Регулярный граф в экспандер с малой потерей в зазоре

- Добавляем к d-регулярному графу G рёбра d_0-экспандера на том же множестве вершин.
- Добавляем к каждой вершине $d + d_0$ петель.
- На добавленных ребрах ограничения всегда выполнены.
- Увеличение размера графа линейное.

Теорема о реберных и алгебраических экспандерах

$$1 - 2\frac{h(G)}{d} \leqslant \frac{\lambda(G)}{d} \leqslant 1 - \frac{h(G)^2}{2d^2}$$

Лемма об экспандеризации

Существует полиномиально вычислимое преобразование $G \mapsto G''$, которое любой граф ограничений переводит в (λ, d'')-экспандер с $\lambda < 1$, размер графа ограничений увеличивается линейно, а

$$\beta_1 \mathrm{UNSAT}(G) \leqslant \mathrm{UNSAT}(G'') \leqslant \mathrm{UNSAT}(G).$$

Регулярный граф в экспандер с малой потерей в зазоре

- Добавляем к d-регулярному графу G рёбра d_0-экспандера на том же множестве вершин.
- Добавляем к каждой вершине $d + d_0$ петель.
- На добавленных ребрах ограничения всегда выполнены.
- Увеличение размера графа линейное.

Теорема о реберных и алгебраических экспандерах

$$1 - 2\frac{h(G)}{d} \leqslant \frac{\lambda(G)}{d} \leqslant 1 - \frac{h(G)^2}{2d^2}$$

Лемма об экспандеризации

Существует полиномиально вычислимое преобразование $G \mapsto G''$, которое любой граф ограничений переводит в (λ, d'')-экспандер с $\lambda < 1$, размер графа ограничений увеличивается линейно, а

$$\beta_1 \text{UNSAT}(G) \leqslant \text{UNSAT}(G'') \leqslant \text{UNSAT}(G).$$

План

1. Увеличение зазора
2. Уменьшение алфавита: локально проверяемые коды
3. Преобразование k-выполнимости в 2-выполнимость
4. Улучшение графа
5. Выбор параметров

Преобразования за одну сводимость удвоения зазора

β_1, β_2, β_3, d, t, k — абсолютные константы.

G	k	V	E	Σ	$\textsc{unsat}(G)$
исходный	2	v	e	$s = 2^k$	γ
улучшение графа	2	$v' = 2e$	$e' \leqslant 4de$	s	$\beta_1\gamma \leqslant \gamma' \leqslant \gamma$
увеличение зазора	2	$v'' = v'$	$e'' \leqslant \leqslant d^{2t+1}e'$	$s'' = = s^{d^{3t}}$	$\gamma' \neq 0 \ \Rightarrow\ \gamma'' \geqslant \geqslant \beta_2\sqrt{t}\min(\gamma', 1/\sqrt{t})$
уменьшение алфавита	k	$M(s)v''$	$M(s)e''$	2	$\beta_3\gamma'' \leqslant \gamma''' \leqslant \gamma''$
уменьшение арности	2	$v''' + +e'''$	ke'''	2^k	$\tilde{\gamma} = \gamma'''$

$$\gamma \neq 0 \ \Rightarrow\ \tilde{\gamma} \geqslant \min\left(\beta_1\beta_2\beta_3\sqrt{t}\,\gamma, \beta_2\beta_3\right)$$

β_1, β_2, β_3, d, t, k — абсолютные константы.

G	k	V	E	Σ	$\mathrm{UNSAT}(G)$
исходный	2	v	e	$s = 2^k$	γ
улучшение графа	2	$v' = 2e$	$e' \leqslant 4de$	s	$\beta_1\gamma \leqslant \gamma' \leqslant \gamma$
увеличение зазора	2	$v'' = v'$	$e'' \leqslant$ $\leqslant d^{2t+1}e'$	$s'' =$ $= s^{d^{3t}}$	$\gamma' \neq 0 \;\Rightarrow\; \gamma'' \geqslant$ $\geqslant \beta_2\sqrt{t}\min(\gamma', 1/\sqrt{t})$
уменьшение алфавита	k	$M(s)v''$	$M(s)e''$	2	$\beta_3\gamma'' \leqslant \gamma''' \leqslant \gamma''$
уменьшение арности	2	$v'''+$ $+e'''$	ke'''	2^k	$\widetilde{\gamma} = \gamma'''$

$$\gamma \neq 0 \;\Rightarrow\; \tilde{\gamma} \geqslant \min\left(\beta_1\beta_2\beta_3\sqrt{t}\,\gamma, \beta_2\beta_3\right)$$

Преобразования за одну сводимость удвоения зазора

β_1, β_2, β_3, d, t, k — абсолютные константы.

G	k	V	E	Σ	$\mathrm{UNSAT}(G)$
исходный	2	v	e	$s = 2^k$	γ
улучшение графа	2	$v' = 2e$	$e' \leqslant 4de$	s	$\beta_1\gamma \leqslant \gamma' \leqslant \gamma$
увеличение зазора	2	$v'' = v'$	$e'' \leqslant \leqslant d^{2t+1}e'$	$s'' = = s^{d^{3t}}$	$\gamma' \neq 0 \;\Rightarrow\; \gamma'' \geqslant \geqslant \beta_2\sqrt{t}\min(\gamma', 1/\sqrt{t})$
уменьшение алфавита	k	$M(s)v''$	$M(s)e''$	2	$\beta_3\gamma'' \leqslant \gamma''' \leqslant \gamma''$
уменьшение арности	2	$v''' + +e'''$	ke'''	2^k	$\tilde{\gamma} = \gamma'''$

$$\gamma \neq 0 \;\Rightarrow\; \tilde{\gamma} \geqslant \min\left(\beta_1\beta_2\beta_3\sqrt{t}\,\gamma, \beta_2\beta_3\right)$$

Преобразования за одну сводимость удвоения зазора

β_1, β_2, β_3, d, t, k — абсолютные константы.

G	k	V	E	Σ	$\text{UNSAT}(G)$
исходный	2	v	e	$s = 2^k$	γ
улучшение графа	2	$v' = 2e$	$e' \leqslant 4de$	s	$\beta_1\gamma \leqslant \gamma' \leqslant \gamma$
увеличение зазора	2	$v'' = v'$	$e'' \leqslant$ $\leqslant d^{2t+1}e'$	$s'' =$ $= s^{d^{3t}}$	$\gamma' \neq 0 \;\Rightarrow\; \gamma'' \geqslant$ $\geqslant \beta_2\sqrt{t}\min(\gamma', 1/\sqrt{t})$
уменьшение алфавита	k	$M(s)v''$	$M(s)e''$	2	$\beta_3\gamma'' \leqslant \gamma''' \leqslant \gamma''$
уменьшение арности	2	$v'''+$ $+e'''$	ke'''	2^k	$\tilde{\gamma} = \gamma'''$

$$\gamma \neq 0 \;\Rightarrow\; \tilde{\gamma} \geqslant \min\left(\beta_1\beta_2\beta_3\sqrt{t}\,\gamma, \beta_2\beta_3\right)$$

Преобразования за одну сводимость удвоения зазора

β_1, β_2, β_3, d, t, k — абсолютные константы.

G	k	V	E	Σ	$\mathrm{UNSAT}(G)$
исходный	2	v	e	$s = 2^k$	γ
улучшение графа	2	$v' = 2e$	$e' \leqslant 4de$	s	$\beta_1\gamma \leqslant \gamma' \leqslant \gamma$
увеличение зазора	2	$v'' = v'$	$e'' \leqslant$ $\leqslant d^{2t+1}e'$	$s'' =$ $= s^{d^{3t}}$	$\gamma' \neq 0 \;\Rightarrow\; \gamma'' \geqslant$ $\geqslant \beta_2\sqrt{t}\min(\gamma', 1/\sqrt{t})$
уменьшение алфавита	k	$M(s)v''$	$M(s)e''$	2	$\beta_3\gamma'' \leqslant \gamma''' \leqslant \gamma''$
уменьшение арности	2	$v'''+$ $+e'''$	ke'''	2^k	$\tilde{\gamma} = \gamma'''$

$$\gamma \neq 0 \;\Rightarrow\; \tilde{\gamma} \geqslant \min\left(\beta_1\beta_2\beta_3\sqrt{t}\,\gamma, \beta_2\beta_3\right)$$

Преобразования за одну сводимость удвоения зазора

β_1, β_2, β_3, d, t, k — абсолютные константы.

G	k	V	E	Σ	$\textsc{unsat}(G)$
исходный	2	v	e	$s = 2^k$	γ
улучшение графа	2	$v' = 2e$	$e' \leqslant 4de$	s	$\beta_1\gamma \leqslant \gamma' \leqslant \gamma$
увеличение зазора	2	$v'' = v'$	$e'' \leqslant$ $\leqslant d^{2t+1}e'$	$s'' =$ $= s^{d^{3t}}$	$\gamma' \neq 0 \ \Rightarrow \ \gamma'' \geqslant$ $\geqslant \beta_2\sqrt{t}\min(\gamma', 1/\sqrt{t})$
уменьшение алфавита	k	$M(s)v''$	$M(s)e''$	2	$\beta_3\gamma'' \leqslant \gamma''' \leqslant \gamma''$
уменьшение арности	2	$v'''+$ $+e'''$	ke'''	2^k	$\tilde{\gamma} = \gamma'''$

$$\gamma \neq 0 \ \Rightarrow \ \tilde{\gamma} \geqslant \min\left(\beta_1\beta_2\beta_3\sqrt{t}\,\gamma, \beta_2\beta_3\right)$$

Преобразования за одну сводимость удвоения зазора

β_1, β_2, β_3, d, t, k — абсолютные константы.

G	k	V	E	Σ	$\textsc{unsat}(G)$
исходный	2	v	e	$s = 2^k$	γ
улучшение графа	2	$v' = 2e$	$e' \leqslant 4de$	s	$\beta_1\gamma \leqslant \gamma' \leqslant \gamma$
увеличение зазора	2	$v'' = v'$	$e'' \leqslant \leqslant d^{2t+1}e'$	$s'' = = s^{d^{3t}}$	$\gamma' \neq 0 \ \Rightarrow \ \gamma'' \geqslant \geqslant \beta_2\sqrt{t}\min(\gamma', 1/\sqrt{t})$
уменьшение алфавита	k	$M(s)v''$	$M(s)e''$	2	$\beta_3\gamma'' \leqslant \gamma''' \leqslant \gamma''$
уменьшение арности	2	$v'''+ +e'''$	ke'''	2^k	$\widetilde{\gamma} = \gamma'''$

$$\gamma \neq 0 \ \Rightarrow \ \tilde{\gamma} \geqslant \min\left(\beta_1\beta_2\beta_3\sqrt{t}\,\gamma, \beta_2\beta_3\right)$$

Преобразования за одну сводимость удвоения зазора

β_1, β_2, β_3, d, t, k — абсолютные константы.

G	k	V	E	Σ	$\textsc{unsat}(G)$
исходный	2	v	e	$s = 2^k$	γ
улучшение графа	2	$v' = 2e$	$e' \leqslant 4de$	s	$\beta_1\gamma \leqslant \gamma' \leqslant \gamma$
увеличение зазора	2	$v'' = v'$	$e'' \leqslant \leqslant d^{2t+1}e'$	$s'' = = s^{d^{3t}}$	$\gamma' \neq 0 \ \Rightarrow \ \gamma'' \geqslant \geqslant \beta_2\sqrt{t}\min(\gamma', 1/\sqrt{t})$
уменьшение алфавита	k	$M(s)v''$	$M(s)e''$	2	$\beta_3\gamma'' \leqslant \gamma''' \leqslant \gamma''$
уменьшение арности	2	$v'''+ +e'''$	ke'''	2^k	$\tilde{\gamma} = \gamma'''$

$$\gamma \neq 0 \ \Rightarrow \ \tilde{\gamma} \geqslant \min\left(\beta_1\beta_2\beta_3\sqrt{t}\,\gamma, \beta_2\beta_3\right)$$

Подбор параметров

Параметры β_1, β_2, β_3, λ, d, t, k.

$$\gamma \neq 0 \;\Rightarrow\; \tilde{\gamma} \geqslant \min(\beta_1\beta_2\beta_3\sqrt{t}\,\gamma, \beta_2\beta_3)$$

1. k возникает как константа в конструкции уменьшения алфавита ($k = 10$).
2. d возникает как константа в конструкции улучшения графа.
3. β_1 зависит от d и от λ, которая возникает в конструкции улучшения графа.
4. β_2 зависит от λ, d, $s = 2^k$.
5. β_3 возникает как константа в конструкции уменьшения алфавита.
6. t выберем больше, чем $\dfrac{4}{\beta_1^2\beta_2^2\beta_3^3}$, тогда $\tilde{\gamma} \geqslant \min(2\gamma, \beta_2\beta_3)$.
7. Порог увеличения зазора $\alpha = \beta_2\beta_3$.

Подбор параметров

Параметры β_1, β_2, β_3, λ, d, t, k.

$$\gamma \neq 0 \;\Rightarrow\; \tilde{\gamma} \geqslant \min(\beta_1\beta_2\beta_3\sqrt{t}\,\gamma, \beta_2\beta_3)$$

1. k возникает как константа в конструкции уменьшения алфавита ($k = 10$).
2. d возникает как константа в конструкции улучшения графа.
3. β_1 зависит от d и от λ, которая возникает в конструкции улучшения графа.
4. β_2 зависит от λ, d, $s = 2^k$.
5. β_3 возникает как константа в конструкции уменьшения алфавита.
6. t выберем больше, чем $\dfrac{4}{\beta_1^2\beta_2^2\beta_3^3}$, тогда $\tilde{\gamma} \geqslant \min\left(2\gamma, \beta_2\beta_3\right)$.
7. Порог увеличения зазора $\alpha = \beta_2\beta_3$.

Подбор параметров

Параметры β_1, β_2, β_3, λ, d, t, k.

$$\gamma \neq 0 \;\Rightarrow\; \tilde{\gamma} \geqslant \min(\beta_1\beta_2\beta_3\sqrt{t}\,\gamma, \beta_2\beta_3)$$

1. k возникает как константа в конструкции уменьшения алфавита ($k = 10$).
2. d возникает как константа в конструкции улучшения графа.
3. β_1 зависит от d и от λ, которая возникает в конструкции улучшения графа.
4. β_2 зависит от λ, d, $s = 2^k$.
5. β_3 возникает как константа в конструкции уменьшения алфавита.
6. t выберем больше, чем $\dfrac{4}{\beta_1^2\beta_2^2\beta_3^3}$, тогда $\tilde{\gamma} \geqslant \min(2\gamma, \beta_2\beta_3)$.
7. Порог увеличения зазора $\alpha = \beta_2\beta_3$.

Подбор параметров

Параметры β_1, β_2, β_3, λ, d, t, k.

$$\gamma \neq 0 \;\Rightarrow\; \tilde{\gamma} \geqslant \min(\beta_1\beta_2\beta_3\sqrt{t}\,\gamma, \beta_2\beta_3)$$

1. k возникает как константа в конструкции уменьшения алфавита ($k = 10$).
2. d возникает как константа в конструкции улучшения графа.
3. β_1 зависит от d и от λ, которая возникает в конструкции улучшения графа.
4. β_2 зависит от λ, d, $s = 2^k$.
5. β_3 возникает как константа в конструкции уменьшения алфавита.
6. t выберем больше, чем $\dfrac{4}{\beta_1^2\beta_2^2\beta_3^3}$, тогда $\tilde{\gamma} \geqslant \min\left(2\gamma, \beta_2\beta_3\right)$.
7. Порог увеличения зазора $\alpha = \beta_2\beta_3$.

Подбор параметров

Параметры β_1, β_2, β_3, λ, d, t, k.

$$\gamma \neq 0 \;\Rightarrow\; \tilde{\gamma} \geqslant \min(\beta_1\beta_2\beta_3\sqrt{t}\,\gamma, \beta_2\beta_3)$$

1. k возникает как константа в конструкции уменьшения алфавита ($k = 10$).
2. d возникает как константа в конструкции улучшения графа.
3. β_1 зависит от d и от λ, которая возникает в конструкции улучшения графа.
4. β_2 зависит от λ, d, $s = 2^k$.
5. β_3 возникает как константа в конструкции уменьшения алфавита.
6. t выберем больше, чем $\dfrac{4}{\beta_1^2\beta_2^2\beta_3^3}$, тогда $\tilde{\gamma} \geqslant \min(2\gamma, \beta_2\beta_3)$.
7. Порог увеличения зазора $\alpha = \beta_2\beta_3$.

Подбор параметров

Параметры β_1, β_2, β_3, λ, d, t, k.

$$\gamma \neq 0 \;\Rightarrow\; \tilde{\gamma} \geqslant \min(\beta_1\beta_2\beta_3\sqrt{t}\,\gamma, \beta_2\beta_3)$$

1. k возникает как константа в конструкции уменьшения алфавита ($k = 10$).
2. d возникает как константа в конструкции улучшения графа.
3. β_1 зависит от d и от λ, которая возникает в конструкции улучшения графа.
4. β_2 зависит от λ, d, $s = 2^k$.
5. β_3 возникает как константа в конструкции уменьшения алфавита.
6. t выберем больше, чем $\dfrac{4}{\beta_1^2\beta_2^2\beta_3^3}$, тогда $\tilde{\gamma} \geqslant \min(2\gamma, \beta_2\beta_3)$.
7. Порог увеличения зазора $\alpha = \beta_2\beta_3$.

Подбор параметров

Параметры β_1, β_2, β_3, λ, d, t, k.

$$\gamma \neq 0 \;\Rightarrow\; \tilde{\gamma} \geqslant \min(\beta_1\beta_2\beta_3\sqrt{t}\,\gamma, \beta_2\beta_3)$$

1. k возникает как константа в конструкции уменьшения алфавита ($k = 10$).
2. d возникает как константа в конструкции улучшения графа.
3. β_1 зависит от d и от λ, которая возникает в конструкции улучшения графа.
4. β_2 зависит от λ, d, $s = 2^k$.
5. β_3 возникает как константа в конструкции уменьшения алфавита.
6. t выберем больше, чем $\dfrac{4}{\beta_1^2\beta_2^2\beta_3^3}$, тогда $\tilde{\gamma} \geqslant \min(2\gamma, \beta_2\beta_3)$.
7. Порог увеличения зазора $\alpha = \beta_2\beta_3$.