Codificação de Rede com Mínimo Overhead Utilizando Códigos de Máxima Distância de Posto

Danilo Silva e Ricardo Bohaczuk Venturelli

***Resumo*— Este artigo investiga a otimização de parâmetros, em particular o tamanho do corpo finito, em sistemas de codificação de rede linear aleatória baseada em gerações, com o objetivo de minimizar o overhead total do sistema. Sabe-se que o principal problema do uso de um corpo finito pequeno é o grande overhead causado por pacotes linearmente dependentes. Neste artigo, é proposta uma abordagem de pré-codificação através de um código de máxima distância de posto, a qual permite essencialmente eliminar este overhead e significativamente reduzir o overhead total do sistema. Um benefício adicional do uso de um corpo finito pequeno é a redução da complexidade de codificação e decodificação. Resultados de simulações são apresentados, os quais confirmam os resultados teóricos obtidos.**

***Palavras-Chave*— Codificação de rede, corpos finitos, códigos de máxima distância de posto, canais matriciais.**

***Abstract*— This paper investigates the parameter optimization, particularly the choice of the finite field, in generation-based random linear network coding systems, with the goal of minimizing the total overhead. It is well-known that the main issue in using a small field is the large overhead due to linearly dependent packets. In this paper, a pre-coding approach is proposed, based on maximum-rank-distance codes, that can virtually eliminate this overhead and significantly reduce the total overhead of the system. An additional benefit of using a small field is the reduction in encoding and decoding complexity. Simulations are presented that validate the theoretical results.**

***Keywords*— Network coding, finite fields, maximum-rank-distance (MRD) codes, matrix channels.**

I. Introdução

Codificação de rede [1]–[5] é um novo paradigma para comunicações em rede que generaliza a técnica de roteamento: ao invés de simplesmente repassar os pacotes recebidos, os nós da rede podem produzir novos pacotes combinando algebricamente os pacotes recebidos. Esta estratégia tem o potencial de evitar congestionamentos e assim atingir a capacidade de multidifusão da rede, ao mesmo tempo em que dispensa o uso de algoritmos de roteamento complexos. A área tem crescido em ritmo acelerado desde seu surgimento em 2000, e tem encontrado aplicações em diversos cenários, tais como redes peer-to-peer, redes sem fio, armazenamento distribuído, etc.

Uma das abordagens mais populares de codificação de rede é a chamada *codificação de rede linear aleatória baseada em gerações* (GRLNC). Em sistemas GRLNC, os nós da rede produzem novos pacotes calculando combinações lineares aleatórias (sobre um corpo finito $\mathbb{F}_q$) dos pacotes recebidos. Os coeficientes usados em tais combinações lineares são armazenados num cabeçalho no próprio pacote, permitindo sua posterior decodificação através da resolução de um sistema de equações lineares. Além disso, a separação de pacotes em *gerações* (conjuntos de k pacotes), de forma que apenas pacotes de uma mesma geração são misturados entre si, permite controlar a complexidade da decodificação, tornando seu uso viável em sistemas práticos [5].

Um dos principais desafios no uso da GRLNC, além da complexidade aritmética envolvida, refere-se ao *overhead* de comunicação intrínseco ao sistema. Devido ao fato de que os pacotes transmitidos são produzidos através de combinações lineares *aleatórias*, existe uma probabilidade não-nula de que o pacote recebido por um nó seja linearmente dependente dos pacotes previamente recebidos por este nó—e portanto, redundante, i.e., não acrescente nenhuma informação nova.

Para reduzir este overhead—chamado aqui de *overhead de dependência linear*— é uma prática comum utilizar um corpo finito de tamanho suficientemente grande, de forma que a probabilidade de dependência linear é significativamente reduzida. O valor mais comumente usado na prática é $q = 256$ [6], enquanto o valor de $q = 2$ é raramente usado em sistemas GRLNC, exceto no caso de dispositivos móveis para os quais a complexidade do uso de um corpo maior não é tolerável.

No entanto, o aumento do tamanho do corpo finito tem impacto negativo em outro overhead: o *overhead devido ao cabeçalho* presente em todo pacote codificado, o qual ocupa pelo menos $k \log_2 q$ bits. Por exemplo, no caso de um pacote de rede típico de cerca de 1500 bytes, com $q = 256$ e gerações de tamanho $k = 100$, este overhead já é superior a 6.6%, chegando a 10% para um pacote de 1KB. Note que decrementar k potencializa outros problemas (pacotes recebidos em excesso após a geração ter sido decodificada) [5], [7], enquanto na maioria dos casos um valor ainda maior de k seria preferível (caso o overhead resultante fosse tolerável). Dessa forma, estes dois overheads, assim como a complexidade das operações em $\mathbb{F}_q$, são considerados alguns dos principais obstáculos à utilização de GRLNC em sistemas práticos.

Neste artigo, é proposta uma nova abordagem para a redução do overhead de dependência linear, a qual é baseada no uso de códigos de máxima distância de posto (MRD) [8]. Códigos MRD são códigos matriciais baseados na métrica de *distância de posto*, os quais tem encontrado diversas aplicações em codificação de rede [9]. A principal contribuição deste artigo é mostrar que, realizando uma pré-codificação da mensagem com um código MRD de taxa apropriada, é possível praticamente eliminar o overhead de dependência linear e significativamente reduzir o overhead total do sistema (para menos de 1% com parâmetros típicos). Além de obter analiticamente o valor ótimo da taxa do código, mostra-se que, quando este valor é utilizado, o tamanho de corpo finito que

Danilo Silva e Ricardo Bohaczuk Venturelli, Departamento de Engenharia Elétrica, Universidade Federal de Santa Catarina, Florianópolis-SC, Brasil, E-mails: danilo@eel.ufsc.br, ricardoxadrez@hotmail.com. Este trabalho foi parcialmente financiado pelo CNPq (482131/2010-1).

minimiza o overhead total é dado por $q = 2$. Este é um resultado aparentemente surpreendente, em contraste com a prática corrente na área, que permite não apenas minimizar o overhead do sistema, mas também simplificar as operações realizadas em todos os nós da rede.

O artigo está organizado da seguinte forma. As Seções II e III apresentam revisões sobre códigos MRD e sistemas GRLNC, respectivamente. A Seção IV apresenta definições e análise de overhead de sistemas GRLNC, com a introdução do conceito de overhead intrínseco. A Seção V introduz a estratégia de pré-codificação MRD e aborda a otimização de parâmetros para minimização do overhead. A Seção VI avalia experimentalmente o emprego da técnica proposta em redes genéricas. Finalmente, a Seção VII apresenta as conclusões do artigo. Provas foram omitidas devido à limitação de espaço.

A. Notação

Seja $\mathbb{F}_q^n$ o espaço vetorial de dimensão n sobre um corpo finito $\mathbb{F}_q$ e seja $\mathbb{F}_q^{n\times m}$ o conjunto de todas as matrizes $n \times m$ com elementos em $\mathbb{F}_q$. A notação $E[X]$ indica o valor esperado de uma variável aleatória X. As funções piso e teto são denotadas por $\lfloor x \rfloor$ e $\lceil x \rceil$, respectivamente.

II. Códigos de Máxima Distância de Posto

A *distância de posto* [8] entre duas matrizes $X, Y \in \mathbb{F}_q^{n\times \ell}$ é definida como $d_{\mathrm{R}}(X,Y) \triangleq \mathsf{posto}(Y - X)$. Seja $d_{\mathrm{R}}(\mathcal{C})$ a *mínima distância de posto* de um código matricial $\mathcal{C} \subseteq \mathbb{F}_q^{n\times \ell}$, isto é, a menor distância de posto entre palavras distintas do código. A cardinalidade de um código matricial é limitada por [8], [10]

$$|\mathcal{C}| \leq q^{\max\{n,\ell\}(\min\{n,\ell\}-d+1)}$$

onde $d = d_{\mathrm{R}}(\mathcal{C})$. Um código que atinge esse limitante com igualdade é chamado de código de *máxima distância de posto* (MRD). Códigos MRD existem para todos os valores de q, n, ℓ e d [8]. Em particular, se $\ell \geq n$, a mínima distância de posto de um código MRD é dada por $d = n - k + 1$, onde $k = \frac{1}{\ell}\log_q |\mathcal{C}|$.

Uma propriedade importante de códigos matriciais, a qual será explorada neste artigo, é sua capacidade de corrigir *apagamentos de posto* [9], [10]. Mais precisamente, se $\mathcal{C} \subseteq \mathbb{F}_q^{n\times \ell}$ possui $d_{\mathrm{R}}(\mathcal{C}) = \mu + 1$, e $A \in \mathbb{F}_q^{m\times n}$ é *qualquer* matriz com $\mathsf{posto}(A) \geq n - \mu$, então o conhecimento do par (A, Y), onde $Y = AX$, permite que $X \in \mathcal{C}$ seja *unicamente* determinado.

Conforme mostrado em [9], no caso dos códigos MRD propostos por Gabidulin [8], a decodificação descrita acima pode ser realizada de forma eficiente, utilizando cerca de $O(\mu^2 n\ell)$ operações em $\mathbb{F}_q$.

III. Codificação de Rede Linear Aleatória Baseada em Gerações

Esta seção apresenta uma revisão sobre codificação de rede linear aleatória baseada em gerações (GRLNC). Um tratamento mais detalhado sobre codificação de rede pode ser encontrado em [11].

Considere uma rede de comunicação modelada por um multigrafo (i.e., um grafo em que arestas paralelas são permitidas) com arestas dirigidas contendo um único nó-fonte e um conjunto de nós-destino. Deseja-se difundir uma mensagem produzida na fonte até cada um dos destinos, um problema conhecido como multidifusão. Assume-se que cada aresta da rede é capaz de transmitir, sem erros, um único pacote de tamanho fixo por unidade de tempo. Canais de maior capacidade são modelados através de arestas paralelas.

Assuma que a mensagem produzida pela fonte é particionada em $K = kL$ pacotes de tamanho P bits, chamados de *pacotes originais*, que por sua vez estão organizados em L conjuntos de k pacotes cada, chamados de *gerações*, correspondendo a um total de $KP = kLP$ bits de mensagem. Seja $\mathbb{F}_q$ um corpo finito de tamanho q, onde q é uma potência de 2, e assuma que $P = \ell \log_2 q$, onde ℓ é um número inteiro, de tal forma que cada pacote original pode ser considerado um vetor em $\mathbb{F}_q^\ell$.

Cada pacote original é formatado com um *cabeçalho de identificação* formado por um identificador da geração à qual o pacote pertence e por um vetor de comprimento k com coeficientes em $\mathbb{F}_q$ chamado de *vetor de codificação global* do pacote. Este vetor é calculado de tal forma que o i-ésimo pacote original de cada geração possui vetor de codificação global com coeficientes nulos exceto por um único 1 na posição i. Assim, após a anexação do cabeçalho—e excetuando-se o identificador da geração—cada pacote original pode ser considerado um vetor em $\mathbb{F}_q^{(k+\ell)}$.

Assuma que cada nó da rede possui um *buffer* para armazenamento de pacotes recebidos. No início da sessão, todos os buffers estão vazios, exceto o buffer da fonte, o qual contém os K pacotes originais (já formatados com o cabeçalho). Em um sistema GRLNC, cada nó da rede, inclusive a fonte, segue o mesmo princípio de operação. A cada nova oportunidade de transmissão de um pacote, o nó realiza as seguintes etapas:

- escolhe uma geração i da qual possui pelo menos um pacote no buffer, de acordo com alguma *estratégia de agendamento de gerações* pré-estabelecida;
- gera r símbolos $a_1, \ldots, a_r \in \mathbb{F}_q$ de forma independente e uniformemente aleatória, onde r é o número de pacotes da geração i presentes no buffer;
- calcula a combinação linear sobre $\mathbb{F}_q$ dada por $\mathbf{v} = a_1\mathbf{u}_1 + \cdots + a_r\mathbf{u}_r$, onde $\mathbf{u}_1, \ldots, \mathbf{u}_r \in \mathbb{F}_q^{k+\ell}$ denotam os pacotes da geração i presentes no buffer;
- transmite o novo pacote $\mathbf{v}$ produzido, mantendo o mesmo identificador da geração i.

Seja $\bar{X}^{(i)} \in \mathbb{F}_q^{k\times \ell}$ uma matriz cujas linhas correspondem aos k pacotes originais da geração i, e seja $X^{(i)} = \begin{bmatrix} I_k & \bar{X}^{(i)} \end{bmatrix}$ a mesma matriz após a anexação dos cabeçalhos. Considere um nó-destino específico que recebe m_i pacotes da geração i, os quais são dispostos como as linhas de uma matriz $Y^{(i)} \in \mathbb{F}_q^{m_i\times(k+\ell)}$. Devido à linearidade da codificação de rede, a matriz $Y^{(i)}$ pode ser expressa como

$$Y^{(i)} = A^{(i)}X^{(i)} = \begin{bmatrix} A^{(i)} & A^{(i)}\bar{X}^{(i)} \end{bmatrix} \tag{1}$$

onde $A^{(i)} \in \mathbb{F}_q^{m_i\times k}$ é a *matriz de transferência* entre fonte e destino correspondente à geração i. Note que a presença do cabeçalho de identificação permite ao destino obter a matriz de transferência $A^{(i)}$, para cada geração, independente da topologia da rede, das escolhas dos coeficientes aleatórios e de possíveis apagamentos de pacotes.

A condição necessária e suficiente para que a geração i possa ser decodificada resolvendo-se o sistema (1) é que $\mathsf{posto}\big(A^{(i)}\big) = k$, sendo que para recuperar a mensagem original da fonte é necessário que todas as gerações sejam decodificadas. A multidifusão é dita bem-sucedida quando todos os destinos conseguem recuperar a mensagem da fonte. Em geral, é sempre possível garantir o sucesso da multidifusão desde que o sistema seja mantido em operação por um tempo suficiente. Dessa forma, novos pacotes chegarão ao receptor ao longo do tempo, o que finalmente produzirá uma matriz $Y^{(i)}$ (e consequentemente também a matriz $A^{(i)}$) de posto k, permitindo a decodificação da geração e posteriormente da mensagem original.

A decodificação dos pacotes originais através da resolução de (1) corresponde, essencialmente, à conversão de $Y^{(i)}$ para forma escalonada reduzida por linhas. A complexidade desse procedimento pode ser calculada como $O(k^2(k+\ell))$ operações em $\mathbb{F}_q$ para cada geração, ou aproximadamente $O(k)$ operações em $\mathbb{F}_q$ por símbolo de mensagem. Vale ressaltar que a complexidade da *codificação*, em um nó que transmite cerca de K pacotes, possui ordem de grandeza semelhante.

É importante observar que, apesar de extremamente útil, a presença do cabeçalho de identificação implica em um pacote maior, e portanto em um *overhead* na transmissão dos coeficientes do cabeçalho, dado por

$$\epsilon_H = \frac{1}{P}(\lceil \log_2 L \rceil + k \log_2 q) = \frac{\lceil \log_2 L \rceil}{P} + k/\ell$$

medido como uma fração do tamanho do pacote.

IV. Overhead de Sistemas GRLNC

Considere um sistema GRLNC utilizado para multidifusão. O overhead total na recepção, para um dado destino, corresponde ao valor esperado da fração de bits em excesso recebidos por este destino em comparação com o número de bits da mensagem original. Para o sistema como um todo, o overhead total na recepção, denotado por ϵ, é definido como a média dos respectivos overheads entre todos os destinos. É fácil mostrar que ϵ pode ser obtido como

$$\epsilon = \epsilon_R + \epsilon_H + \epsilon_R\epsilon_H \leq \epsilon_R + \epsilon_H + (\epsilon_R + \epsilon_H)^2/4$$

onde ϵ_R, chamado de *overhead devido à recepção de pacotes redundantes* é definido como

$$\epsilon_R \triangleq \frac{E[M]}{K} - 1$$

e M é o número de pacotes recebidos por um destino até que a decodificação se torne possível (isto é, $\mathsf{posto}\big(A^{(i)}\big) = k$ para todo i). Note que, na definição acima, o valor esperado incorpora também a média entre todos os destinos.

A. Overhead Intrínseco

Observa-se que o overhead devido a pacotes redundantes pode ser separado em duas partes, $\epsilon_R = \epsilon_D + \epsilon_G$. O *overhead devido à dependência linear*, denotado por ϵ_D, refere-se a pacotes recebidos que *poderiam* ser inovadores (isto é, linearmente independentes dos demais pacotes recebidos da mesma geração), mas que, por causa do tamanho do corpo finito, acabam sendo linearmente dependentes. Por exemplo, no caso de uma rede contendo apenas fonte e destino, a probabilidade de que próximo pacote recebido seja redundante quando o destino já possuir r pacotes linearmente independentes é dada por q^{r-k}, a qual decresce rapidamente com o aumento de q, se $r < k$.

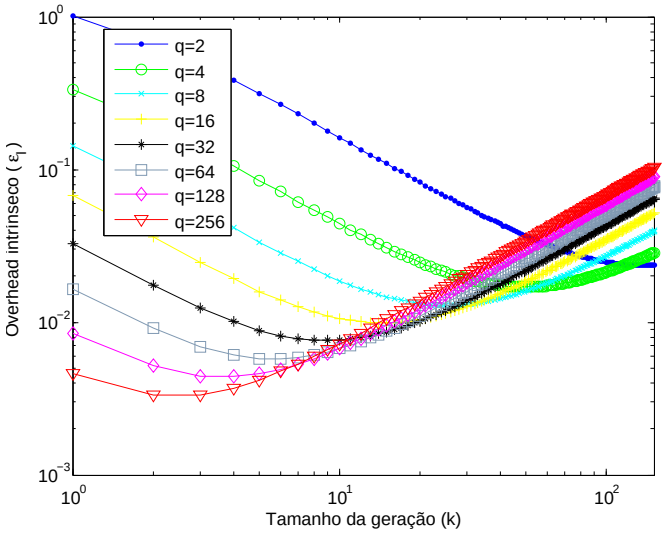

Fig. 1. Overhead intrínseco ϵ_I em função de k e q para um sistema RLNC (com $L = 1$) aplicado a um rede com 2 nós.

Por outro lado, o *overhead devido à geração completa*, denotado por ϵ_G, refere-se aos pacotes recebidos após a geração correspondente ter sido completamente decodificada, e portanto independem do tamanho do corpo finito. Este overhead é causado por imperfeições na estratégia de agendamento de gerações, de forma que um nó continua a transmitir pacotes de uma geração já decodificada pelo destino, ao invés de prosseguir para uma geração diferente.

Matematicamente, define-se $\epsilon_D \triangleq \frac{1}{K}\sum_{i=1}^{L} E[M_i^D]$ e $\epsilon_G \triangleq \frac{1}{K}\sum_{i=1}^{L} E[M_i^F]$, onde M_i^D e M_i^F denotam o número de pacotes redundantes da geração i recebidos, respectivamente, antes e depois da geração ter sido completada.

É conveniente definir o conceito de *overhead intrínseco* de um sistema GRLNC como sendo $\epsilon_I \triangleq \epsilon_D + \epsilon_H$, uma vez que este overhead depende apenas de parâmetros básicos do sistema, independendo da estratégia específica de agendamento de gerações. Assim, temos que $\epsilon \leq \epsilon_G + \epsilon_I + (\epsilon_G + \epsilon_I)^2/4$.

A Fig. 1 mostra a variação de ϵ_I em função de k para vários valores de q, em uma rede com apenas fonte e destino, assumindo um pacote de tamanho[1] $P = 1470 \cdot 8$ bits. Pode-se observar que, à medida que k aumenta, o valor ótimo de q tem de diminuir para reduzir ϵ_H, enquanto para k pequeno o valor ótimo de q precisa ser grande para reduzir ϵ_D.

V. Minimizando o Overhead com Códigos MRD

Esta seção apresenta uma abordagem de pré-codificação para sistemas GRLNC cujo objetivo é minimizar o overhead

[1]Este valor específico de P foi escolhido pois é da ordem de 1500 bytes e é múltiplo de todos os inteiros entre 2 e 8, o que facilita os cálculos.

intrínseco. A análise apresentada assume uma matriz de transferência $A^{(i)}$ uniformemente distribuída, uma hipótese que é satisfeita no caso de uma rede *single-hop* (fonte diretamente conectada aos destinos, sem nós intermediários). Uma extensão para redes mais gerais é descrita na Seção VI.

A. Esquema de Pré-Codificação

Assuma que[2] $k \leq \ell$ e seja n tal que $k \leq n \leq \ell$. Seja $\mathcal{C} \subseteq \mathbb{F}_q^{n\times\ell}$ um código MRD com $d_{\mathrm{R}}(\mathcal{C}) = n-k+1$. Suponha que os k pacotes originais de cada geração i sejam pré-codificados (através de um mapeamento injetivo) em uma palavra-código matricial $\bar{X}^{(i)} \in \mathcal{C}$. (Assim, em comparação com o esquema da Seção III, a matriz $\bar{X}^{(i)}$ agora possui n linhas ao invés de k, onde as $n-k$ linhas adicionais correspondem à redundância do pré-codificador.) Consequentemente, os primeiros m_i pacotes pertencentes a uma geração i recebidos por um destino são dados por

$$Y^{(i)} = \begin{bmatrix} A^{(i)} & A^{(i)}\bar{X}^{(i)} \end{bmatrix}$$

onde $A^{(i)} \in \mathbb{F}_q^{m_i\times n}$ é a matriz de transferência da geração i. Note que, devido à capacidade dos códigos MRD de corrigir apagamentos de posto, a decodificação da geração i pode ser realizada imediatamente após ser obtido $\mathsf{posto}\big(A^{(i)}\big) = k$.

B. Overhead Intrínseco

Para permitir a pré-codificação descrita acima, o cabeçalho de identificação dos pacotes deve ser alongado de forma a acomodar os $n \geq k$ coeficientes do vetor de codificação. Assim, o overhead de cabeçalho torna-se

$$\epsilon_H = \frac{1}{P}(\lceil \log_2 L \rceil + n\log_2 q) = \frac{\lceil \log_2 L \rceil}{P} + n/\ell.$$

Seja $R_i(m_i) \triangleq \min\{\mathsf{posto}\big(A^{(i)}\big), k\}$ o posto acumulado na geração i imediatamente após a recepção do m_i-ésimo pacote da geração i, saturando em k quando a geração pode ser decodificada. Modelando R_i como uma cadeia de Markov, e assumindo que cada nova linha de $A^{(i)}$ é gerada independentemente e uniformemente sobre $\mathbb{F}_q^n$, é possível obter o seguinte resultado.

Teorema 1: $\epsilon_D = \dfrac{1}{k}\displaystyle\sum_{r=0}^{k-1} \frac{1}{q^{n-r}-1}$.

C. Otimização da Taxa do Código

Seja $\mu = n-k$ e denote por

$$\epsilon_I(\mu) \triangleq \frac{\lceil \log_2 L \rceil}{P} + \frac{k+\mu}{\ell} + \frac{1}{k}\sum_{i=1}^{k} \frac{1}{q^{\mu+i}-1}$$

o overhead intrínseco em função de μ. Observando que $\epsilon_I(\mu)$ é uma função convexa, é possível mostrar o seguinte resultado.

Teorema 2: O argumento μ^* que minimiza $\epsilon_I(\mu)$ é dado pelo maior inteiro μ tal que

$$(q^{\mu}-1)^{-1} - (q^{\mu+k}-1)^{-1} \geq k/\ell$$

[2]Note que, para $k > \ell$, o overhead de cabeçalho já é superior a 100%.

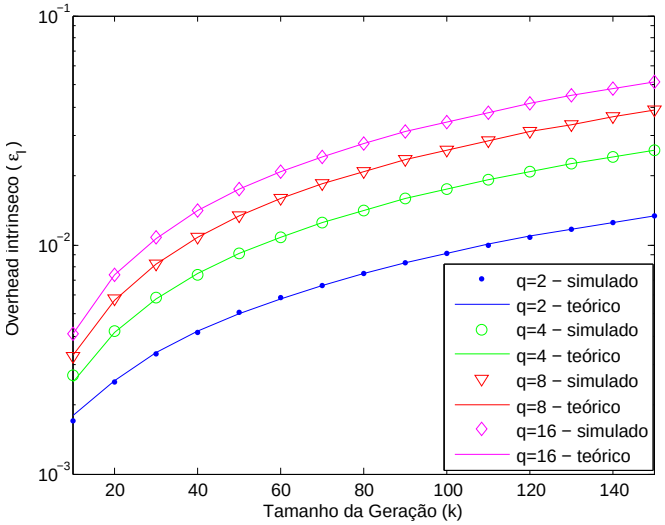

Fig. 2. Overhead intrínseco otimizado, em função de k e q, para um sistema GRLNC com pré-codificação MRD aplicado a um rede com 2 nós. Os resultados de simulação foram obtidos com 100 iterações.

o que pode ser aproximado por

$$\mu^* \approx \left\lfloor \log_q\left(1+\ell/k\right) \right\rfloor.$$

Além disso, pode-se mostrar que o acréscimo em $\epsilon_I(\mu^*)$ caso seja usada a aproximação acima é sempre inferior a $k^{-1}((1+\ell/k)^k-1)^{-1}$, o que converge para 0 rapidamente em função de k, e pode ser considerado desprezível para $k > 1$.

A Fig. 2 mostra o comportamento de $\epsilon_I(\mu^*) - \lceil \log_2 L \rceil/P$ em função de k. Tal comportamento se mantém para quaisquer valores de P (essencialmente deslocando o gráfico para baixo com o aumento de P). Conclui-se que o tamanho de corpo que minimiza $\epsilon_I(\mu^*)$ é dado por $q = 2$.

D. Complexidade

Conforme mencionado na Seção II, a decodificação de um código MRD pode ser realizada com aproximadamente $O(\mu^2)$ operações em $\mathbb{F}_q$ por símbolo de mensagem. Note que μ^* é decrescente com k (em particular, $\mu^* \leq 7$ para $k \geq 47$, $q = 2$ e $P = 1470 \cdot 8$ bits). Vale mencionar que todas as operações envolvidas (re-codificação GRLNC nos nós intermediários e decodificação GRLNC e MRD nos destinos) são significativamente mais simples quando $q = 2$ do que quando $q = 2^8$, o que mais do que compensa a complexidade adicional da decodificação MRD.

VI. Extensão para Redes Mais Complexas

No caso de redes *multi-hop*, a hipótese de que $A^{(i)}$ é uniforme pode se tornar inválida. Por exemplo, no caso de um destino que recebeu $s \leq r$ pacotes linearmente independentes vindos de um nó intermediário, que por sua vez possui apenas $r < k$ pacotes linearmente independentes presentes em seu buffer, é fácil ver que o próximo pacote recebido pelo destino, vindo do nó intermediário, será redundante com probabilidade igual a q^{s-r}, independentemente de ter sido usada pré-codificação MRD. De fato, a pré-codificação MRD só demonstra sua utilidade quando $r \geq k$, o que só ocorre próximo ao final da recepção da geração correspondente.

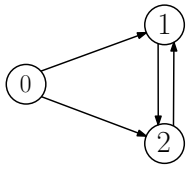

Fig. 3. Rede com fonte (nó 0) e dois destinos (nós 1 e 2).

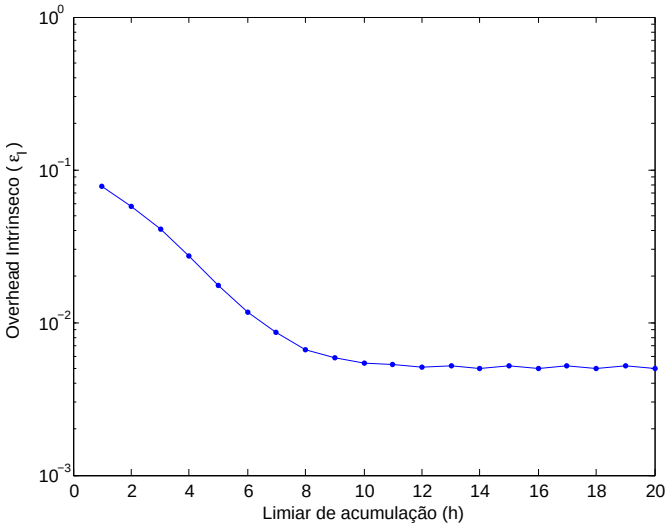

Fig. 4. Overhead intrínseco otimizado, em função de h, para um sistema GRLNC com $q = 2$, aplicado à rede da Fig. 3. Foram utilizadas 1000 iterações.

Para evitar o problema descrito acima, propomos que os nós intermediários devam seguir uma *política de acumulação*: cada nó deve transmitir pacotes de uma geração *somente após* ter acumulado nesta geração um posto maior ou igual a um *limiar de acumulação* h. Esta estratégia garante (sob certas condições de funcionamento da rede) que teremos, no exemplo acima, $r - s \geq h$, e consequentemente uma probabilidade de redundância suficientemente pequena.

Vale mencionar que o atraso decorrente de tal política de acumulação é amortizada com o número de gerações (pois a segunda geração começa a ser acumulada enquanto a primeira geração ainda está sendo concluída, e assim por diante) e portanto tem impacto praticamente desprezível em sistemas GRLNC com valores de parâmetros típicos.

As simulações abaixo foram realizadas para a rede da Fig. 3. A Fig. 4 mostra o overhead intrínseco ϵ_I em função de h, assumindo $q = 2$ e que o valor de μ ótimo é utilizado. A Fig. 5 mostra o overhead intrínseco em função de k para a abordagem proposta (com $q = 2$, $h = 10$ e $\mu = \mu^*$) em comparação com a abordagem tradicional ($q = 256$, $h = 1$ e $\mu = \mu^* = 0$). Estes resultados mostram que, mesmo em redes *multi-hop*, a abordagem proposta permite uma redução de overhead significativa em comparação com a abordagem tradicional.

VII. Conclusões

Neste artigo, apresentamos uma estratégia de pré-codificação MRD que pode ser usada em conjunto com qualquer sistema GRLNC para praticamente eliminar o overhead

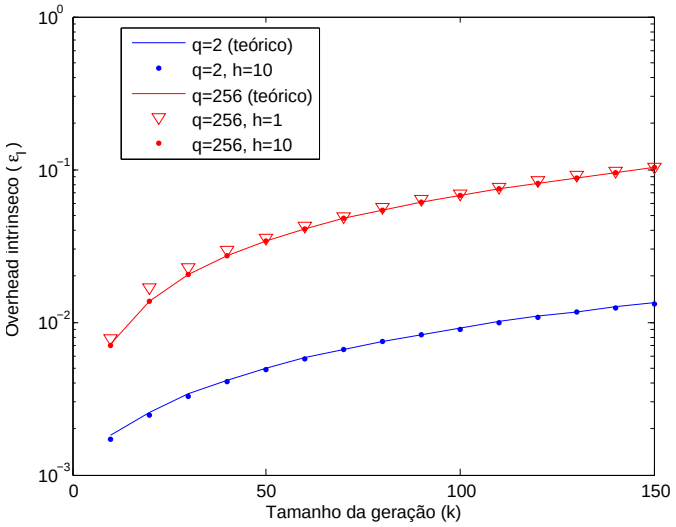

Fig. 5. Overhead intrínseco otimizado, em função de k, para um sistema GRLNC com $q = 2$ e $h = 10$ em comparação com $q = 256$ e $h = 10$, aplicado à rede da Fig. 3. Foram utilizadas 100 iterações.

de dependência linear, e consequentemente reduzir significativamente o overhead intrínseco do sistema. Em particular, é apresentada uma análise que permite encontrar o valor ótimo da taxa de código, assim como o tamanho ótimo do corpo finito—surpreendentemente, este último é obtido como $q = 2$ para todos os cenários investigados. Este resultado permite, simultaneamente, reduzir tanto o overhead quanto a complexidade total do sistema.

Trabalhos futuros envolverão uma avaliação experimental das técnicas propostas aplicadas a redes mais complexas.

Referências

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[2] S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 371–381, Feb. 2003.

[3] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Trans. Netw.*, vol. 11, no. 5, pp. 782–795, Oct. 2003.

[4] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.

[5] P. A. Chou, Y. Wu, and K. Jain, "Practical network coding," in *Proc. Allerton Conf. on Comm., Control, and Computing*, Monticello, IL, Oct. 2003, pp. 40–49.

[6] H. Shojania and B. Li, "Pushing the envelope: Extreme network coding on the GPU," in *Proc. 29th IEEE Int. Conf. Distributed Computing Systems ICDCS '09*, 2009, pp. 490–499.

[7] Z. Liu, C. Wu, B. Li, and S. Zhao, "UUSee: Large-scale operational on-demand streaming with random network coding," in *Proc. IEEE INFOCOM*, 2010, pp. 1–9.

[8] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Probl. Inform. Transm.*, vol. 21, no. 1, pp. 1–12, 1985.

[9] D. Silva, "Error control for network coding," Ph.D. thesis, University of Toronto, Toronto, Canada, 2009.

[10] D. Silva, F. R. Kschischang, and R. Kötter, "A rank-metric approach to error control in random network coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 3951–3967, 2008.

[11] C. Fragouli and E. Soljanin, "Network coding fundamentals," *Foundations and Trends in Networking*, vol. 2, no. 1, pp. 1–133, 2007.